# Videoconferencing Design Guide

# Draft 1.3

# 6/18/01

Author:
Alan Glowacki

# Contents:

## Chapter 1

**H.323 Introduction**

## Chapter 2

**Design Model Introduction**

## Chapter 3

**Campus Infrastructure**

## Chapter 4

**WAN Infrastructure**

## Chapter 5

**WAN QoS**

## Chapter 6

**Dial Plan Architecture**

## Chapter 7

**Call Routing**

## Chapter 8

**Cisco Video Infrastructure Components**

## Chapter 9

# Chapter 1:

# H.323 Introduction:

This chapter provides an overview of the H.323 standard, and the video infrastructure components used to build an H.323 videoconferencing network. This chapter will give you a basic understanding of the H.323 video standard and infrastructure components needed for this document.

This Chapter includes the following sections:

- What is H.323?
- Why H.323 Videoconferencing?
- H.323 Infrastructure Components

## What is H.323?

The H.323 standard provides a foundation for audio, video, and data communications across IP-based networks. H.323 is an umbrella recommendation from the International Telecommunications Union (ITU) that sets standards for multimedia communications over Local Area Networks (LANs). The H.323 standard is part of a larger range of videoconferencing standards (H.32X) for videoconferencing over different network mediums. H.320 supports videoconferencing over ISDN, H.321 supports videoconferencing over ATM, H.324 supports videoconferencing over standard POTS lines, and H.323 supports videoconferencing over IP LANs. The H.323 specification is made up of multiple protocols. Two of the main protocols are defined below. Table 1-1 defines some of the standards supported by the H.323 specification.

- H.245 control signaling is used to exchange end-to-end control messages. These control messages carry information related to the following:

  1. Capabilities exchange
  2. Opening and closing of logical channels used to carry media streams
  3. Flow-control messages
  4. General commands and indications

- H.225 is used for registration, admission and status (RAS), which is the protocol used between H.323 devices and the gatekeeper for device registration. The RAS protocol is used to perform registration, admission control, bandwidth utilization updates, status and disengagement procedures between H.323 devices and the gatekeeper. H.225 is also used during call setup to open a call-signaling channel using standard Q.931 messaging protocol.

## Table 1-1

| | |
|---|---|
| H.225 | RAS, Call Setup and Tear Down (Q.931 call establishment) |
| H.245 | Call Control Messaging |
| H.261<br>H.263 | Video Formats |
| G.711<br>G.722<br>G.723<br>G.728 | Audio Formats |

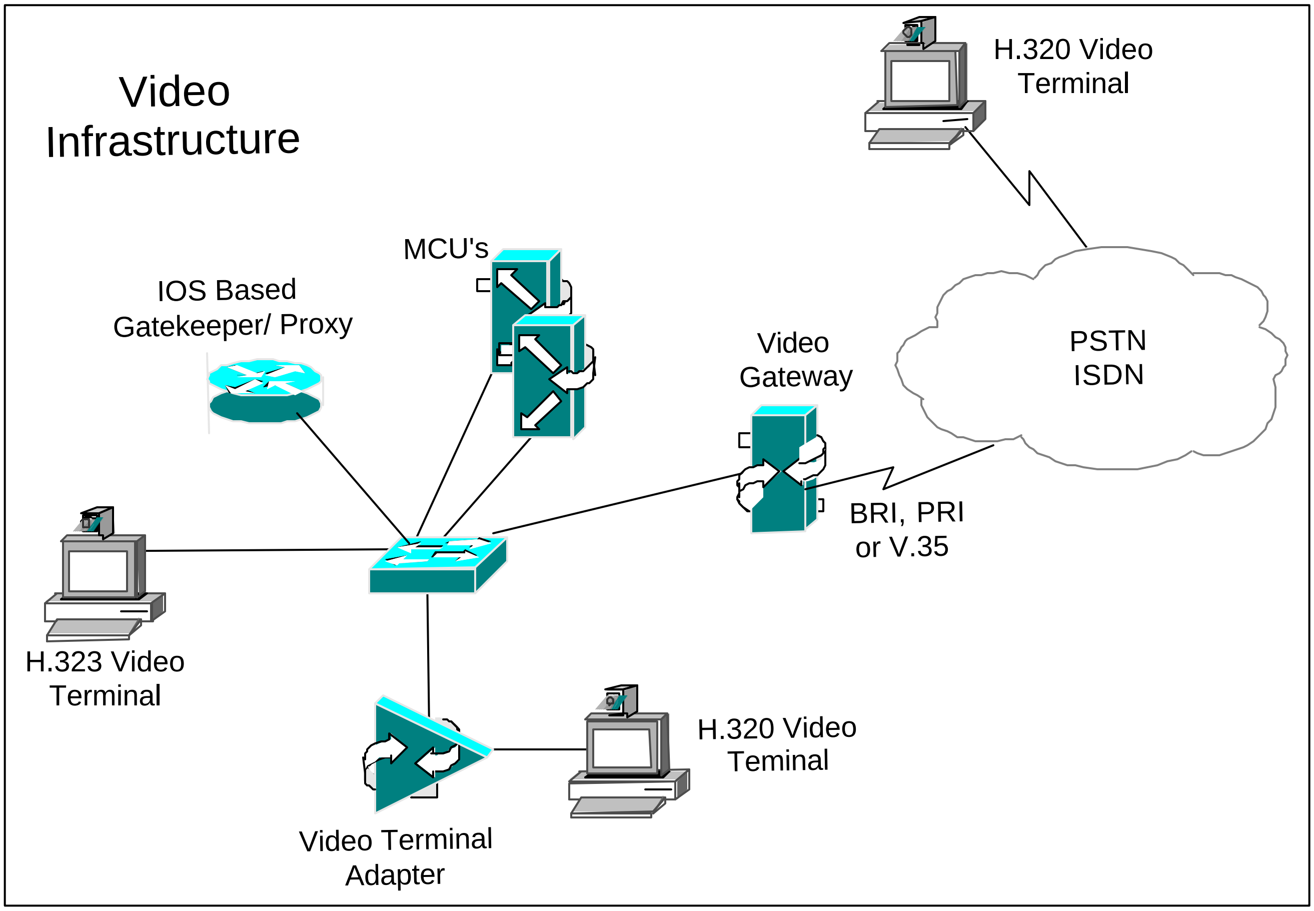
# Why H.323 Videoconferencing?

Historically, videoconferencing was done primarily over ISDN and Time Division Multiplexed networks (H.320). Running interactive video over data networks was not an option due to its shared media characteristics, connection-less nature, and no availability of guaranteed data flows. With the introduction of switched 10/100 Mbps networks, high end routers and layer two and three QoS, delivering interactive video over IP is now reality. Today there is a large installed base of H.320 that incurs large monthly access and switched usage charges. With the current advances to the IP networks, it is now possible to run interactive video over an IP network saving customers thousands of dollars a month by converging voice, video and data traffic over a common path. Costs drop even further as videoconferencing terminals no longer need to support complex network aggregation devices such as IMUXs and can instead rely on simple Ethernet NICs for network connectivity. H.323 builds on top of existing IP data networks, ultimately saving money and scaling to larger deployments. The resulting drop in cost per seat is expected to cause an exponential increase in the number of H.323 terminals deployed as users move video conferencing assets from shared areas such as conference rooms to the user desktop. Distance Learning and Business Meetings are two common applications that can be deployed cost effectively with H.323 over IP data networks.

# H.323 Network Components:

There are five components that make up an H.323 videoconferencing network. These five components are 1.) Video Terminals, 2.) Gatekeepers, 3.) Gateways, 4.) Multipoint conference Units (MCU), and 5.) Proxies. Cisco offers product solutions for all of the above components except video terminals, which are covered in detail in Chapter 8 Video Infrastructure. Figure 1-1 illustrates a H.323 network.

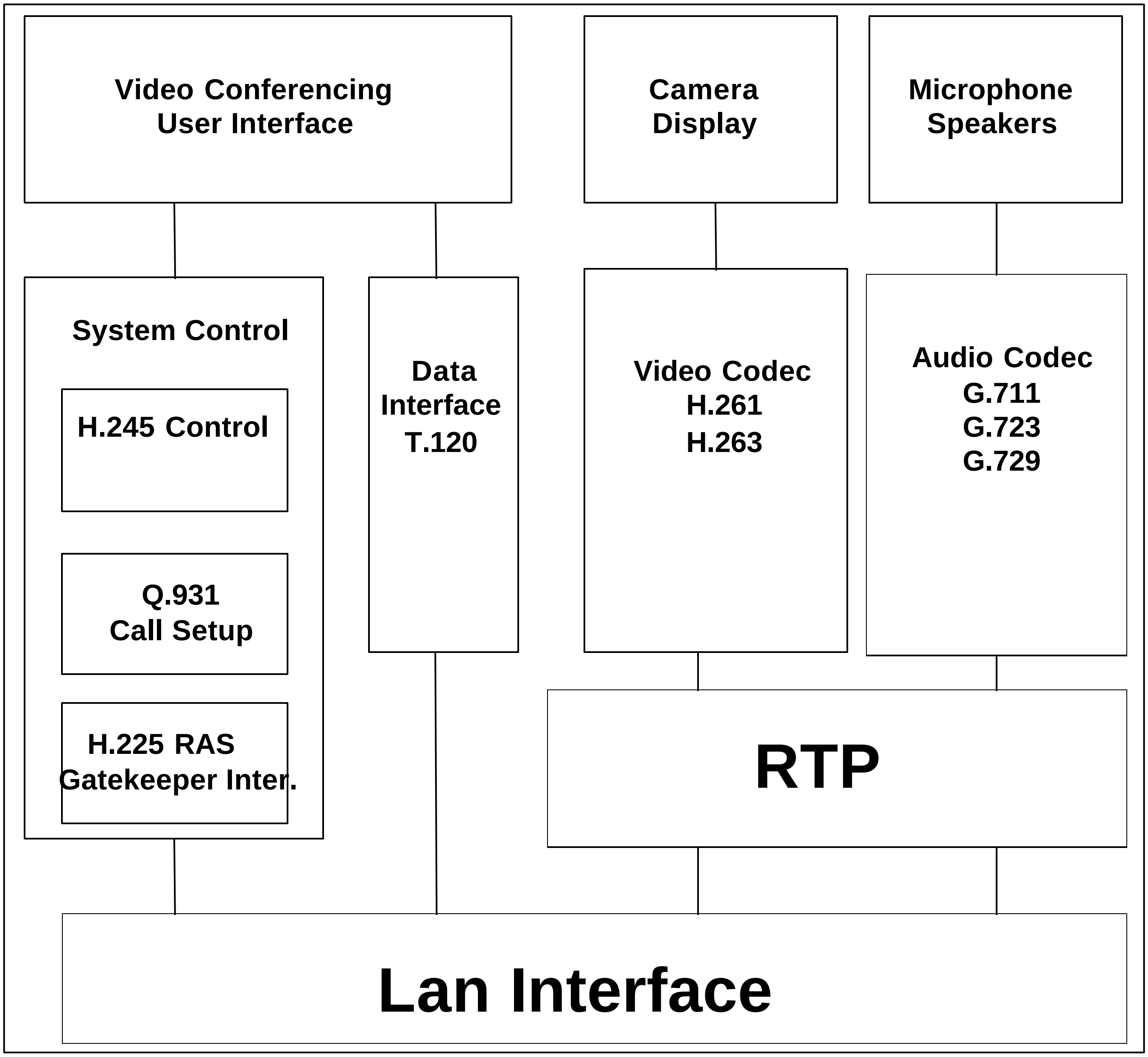
## Figure 1-1


Video
Infrastructure
H.320 Video
Terminal
MCU's
IOS Based
Gatekeeper/ Proxy
Video
Gateway
PSTN
ISDN
BRI, PRI
or V.35
H.323 Video
Terminal
H.320 Video
Teminal
Video Terminal
Adapter

## Video Terminals:

Video Terminals come in multiple form factors including video systems installed on PCs, as a stand-alone desktop terminals, and group-focused shared conference room devices. Figure 1-2 illustrates the components in an H.323 video terminal.

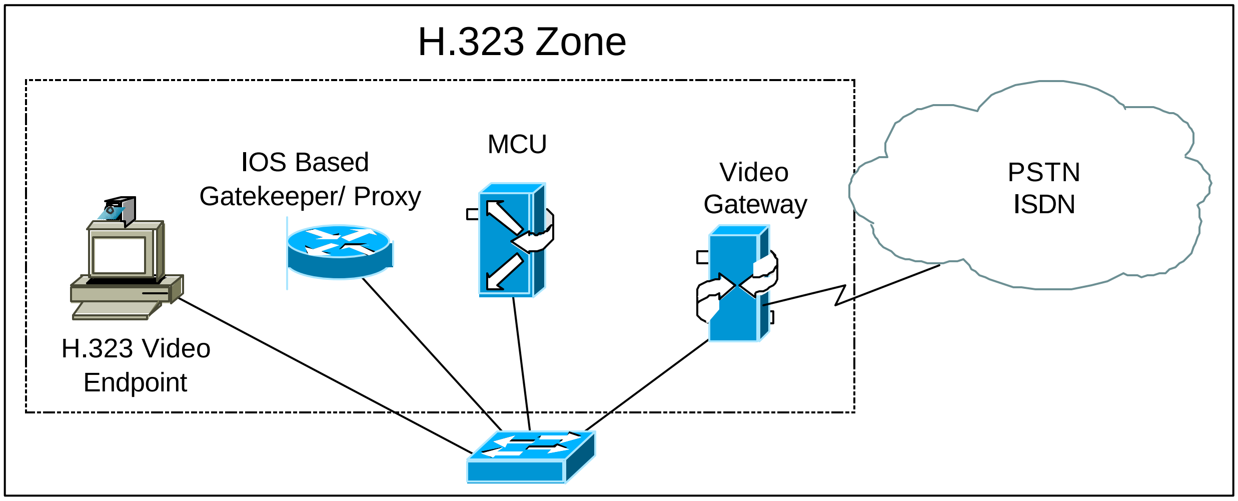
### Figure 1-2



# Gatekeeper:

Gatekeeper is one of the most important components of an H.323 videoconferencing network. While the H.323 standard lists this device as optional, scalable video networks cannot be built without the application controls this device provides. Each video infrastructure component registers with the gatekeeper. The gatekeeper performs all address resolution, bandwidth management, admission control, zone management, and routing of intra and inter-zone calls. A zone is a logical grouping of H.323 infrastructure components managed by a single gatekeeper. Zones are not dependent on physical network topology or IP subnets. Zones may span one or more network segments or IP subnets, and are simply a logical grouping of devices registered to a single gatekeeper. As such, zones can be defined based on geographical proximity, bandwidth availability or other criteria. The most fundamental function of a Gatekeeper is to provide address resolution, allowing terminals, gateways, and MCUs to be addressed using the international E.164 Address standard and/or an H.323 alias. Each endpoint that is registered to a Gatekeeper must be assigned a unique E.164 address (numeric Identifier). As a result, zone prefixes are used in the H.323 video network to uniquely identify zones. This is similar to an area code in the telephony world. Throughout this paper we will deal with example topologies that are based on single zone and multi zone configurations. Figure 1-3 illustrates a single zone.

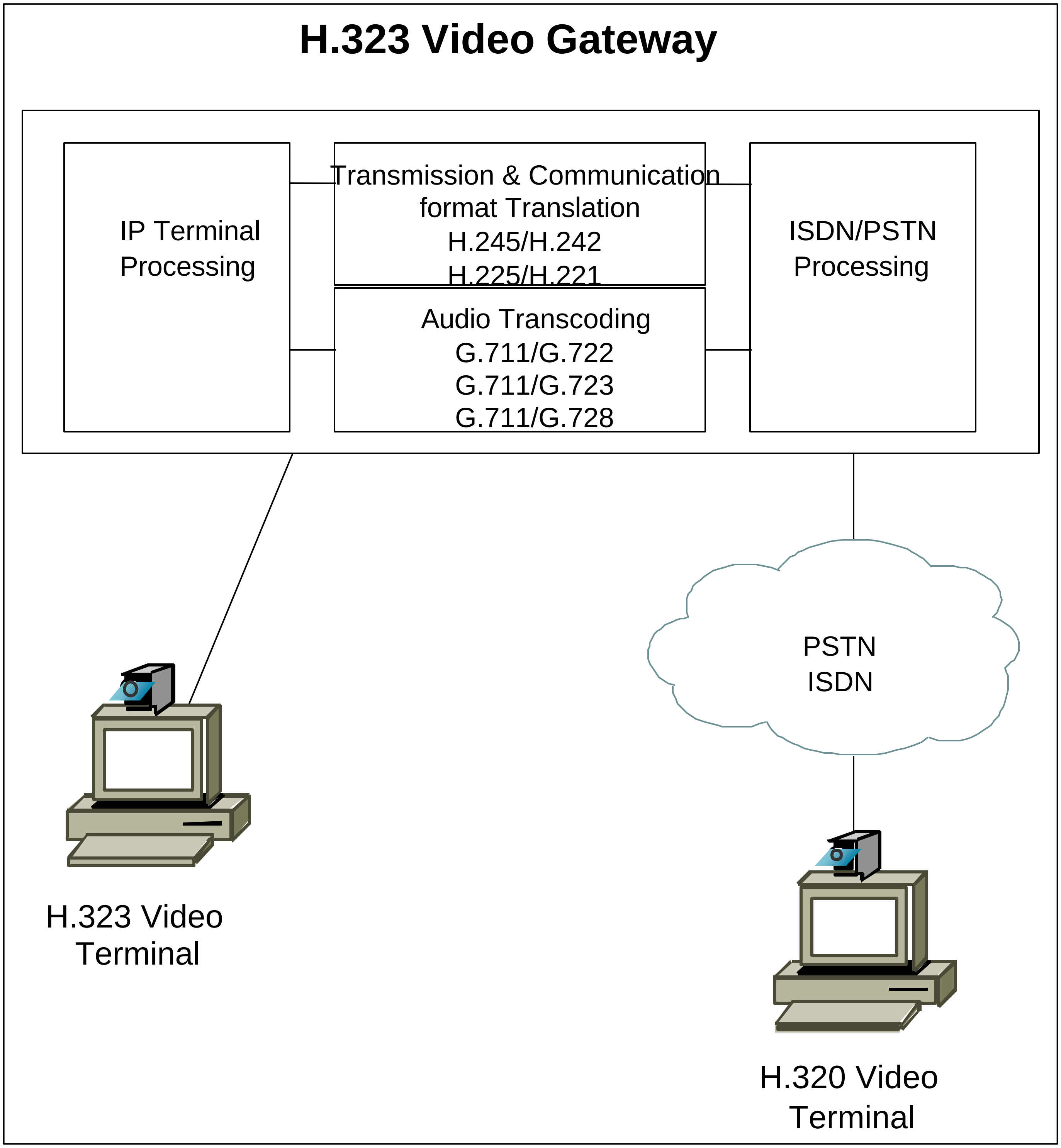
## Figure 1-3



# Gateway:

Gateways provide interoperability between H.323 elements and an installed base of H.320 units. The H.323 gateway allows H.323 video terminals to communicate with other H.32X video terminals, such as H.320 and H.321 video terminals. Video gateways perform translation between different protocols, audio encoding formats and video encoding formats that may be used by the various H.32x standards. For example, the ISDN H.320 standard uses the H.221 protocol for signaling, while the H.323 standard uses H.225. The Gateway must translate between these two protocols to allow devices of different network mediums and protocols to communicate with each other. Figure 1-4 illustrates a gateways roll in an H.323 video network.

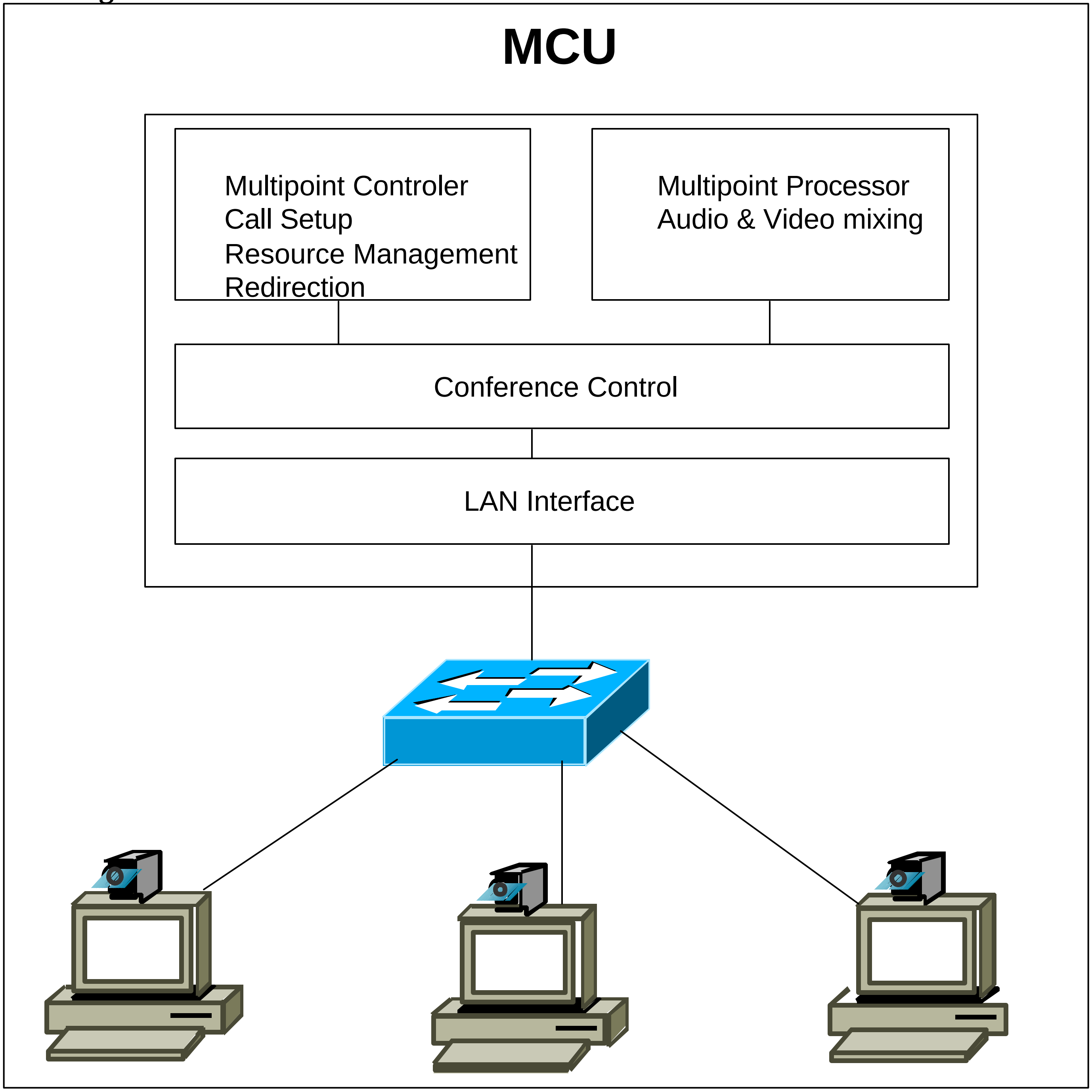
**Figure 1-4**


H.323 Video Gateway
IP Terminal Processing
Transmission & Communication format Translation
H.245/H.242
H.225/H.221
Audio Transcoding
G.711/G.722
G.711/G.723
G.711/G.728
ISDN/PSTN Processing
PSTN
ISDN
H.323 Video Terminal
H.320 Video Terminal

## Multipoint Conference Units (MCU):

Video terminals are generally point-to-point devices allowing only two participants per conversation. A multipoint conference unit (MCU) allows videoconferences to be extended to three or more participants. An MCU consists of a multipoint controller (MC) and a multipoint processor (MP). The MC manages all call setup control functions and conference resources, as well as managing the opening and closing of media streams. The MP will process audio and video media streams only. Cisco MCUs can be stacked to create more conferences or cascaded to create larger conferences. Stacking and cascading is covered in detail in Chapter 8 Video Infrastructure. Figure 1-5 illustrates the function of an MCU

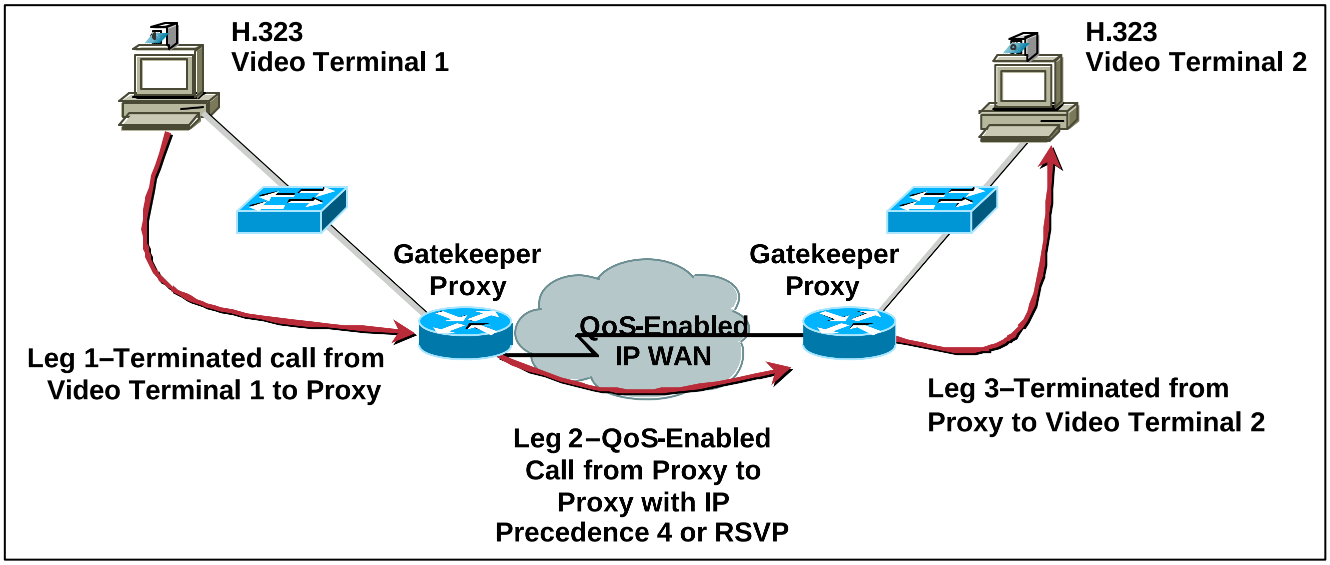
**Figure 1-5**



## Proxy:

A proxy is a call-processing agent that terminates H.323 calls from a local LAN or "zone" and establishes sessions with H.323 endpoints located in different LANs or "zones." In so doing, the proxy provides network administrators with the ability to set and enforce quality of service (QoS) on inter-zone segments. The proxy also provides a method of identifying H.323 videoconferencing connections for tunneling through firewalls and NAT (Network Address Translation) environments. Figure 1-6 illustrates a proxied call over a WAN link.

### Figure 1-6



# Chapter 2:

# Design Model Introduction:

This chapter provides an overview of four basic design models that will be covered in detail throughout this document. This overview provides basic design criteria and guidance for selecting the correct deployment model. The following chapters will build on the four basic models introduced in this chapter.

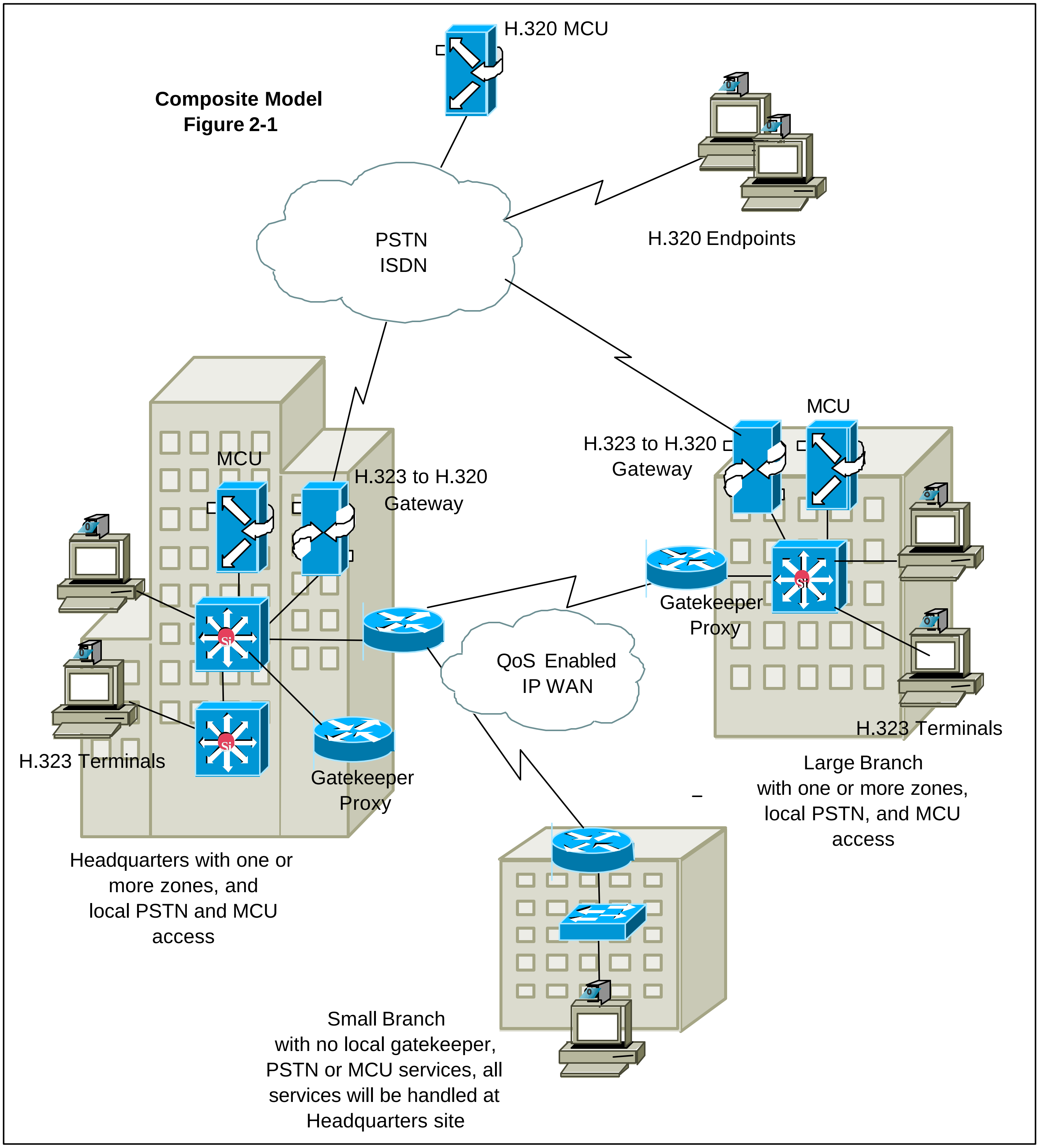
This chapter includes the following sections:

- Composite Design Model
- Campus Single Zone
- Campus Multi Zone
- WAN Single Zone
- WAN Multi Zone

## Composite Design Model

Figure 2-1 shows a composite drawing that encomp asses all of the design models that will be discussed in this guide. All designs discussed in this guide are supported with the current shipping product.

## Figure 2-1


H.320 MCU
Composite Model
Figure 2-1
PSTN
ISDN
H.320 Endpoints
MCU
H.323 to H.320
Gateway
H.323 to H.320
Gateway
MCU
Gatekeeper
Proxy
QoS Enabled
IP WAN
H.323 Terminals
Gatekeeper
Proxy
H.323 Terminals
Large Branch
with one or more zones,
local PSTN, and MCU
access
Headquarters with one or
more zones, and
local PSTN and MCU
access
Small Branch
with no local gatekeeper,
PSTN or MCU services, all
services will be handled at
Headquarters site

Overall goals of a Cisco based H.323 video network.

- End to end IP video connectivity across the corporate infrastructure providing "business quality" transmission ("Business quality" video is defined as 30 frames per second operation with a minimum of CIF resolution and G.711 audio.  Typically, this requires 384kbps of application bandwidth for most video terminals)
- High availability with low latency and Jitter (delay variability) – i.e., Quality of Service
- Reduced ISDN costs by eliminating the need for ISDN attachments directly to video terminals
- PSTN access to legacy H.320 systems through shared gateway resources
- Multipoint calling available through MCUs
- Conservation of WAN bandwidth by distributing MCU and gateway resources across the IP infrastructure
- Lower total cost of ownership for the video network by utilizing current IP infrastructure
- Manageability of multiple H.323 elements in a distributed network topology

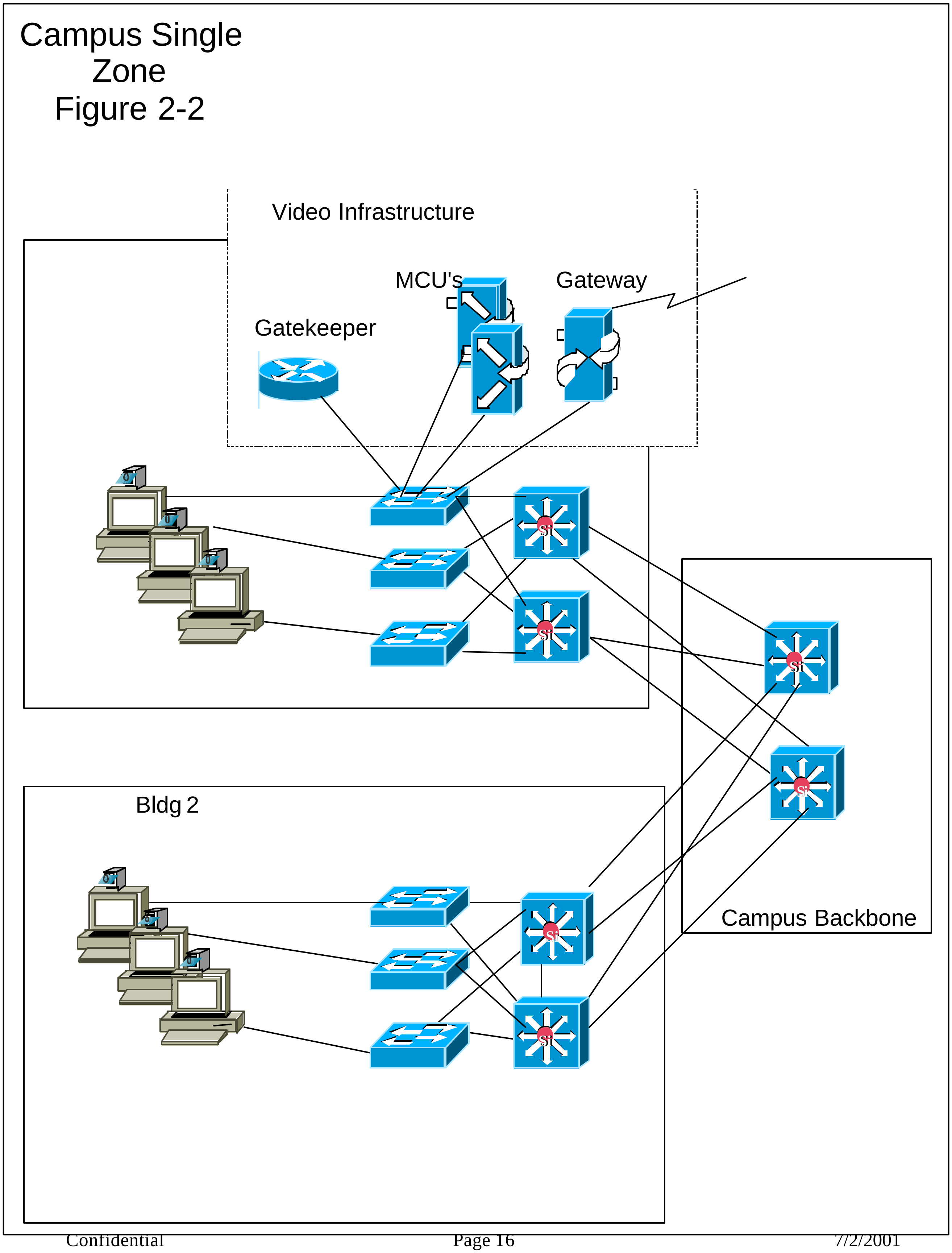
There are four basic design models in an H.323 video network based on Cisco IP/VC and IOS gatekeeper products.

- Campus single zone
- Campus multi zones
- WAN single zone
- WAN multi zones

# Campus single zone:

Figure 2-2 illustrates an H.323 network in a campus environment configured with a single zone.  This is the most basic design model to implement and will be used in pilot installs and smaller video environments.

**Figure 2-2**


Campus Single Zone Figure 2-2
Video Infrastructure
MCU's
Gateway
Gatekeeper
Bldg 2
Campus Backbone

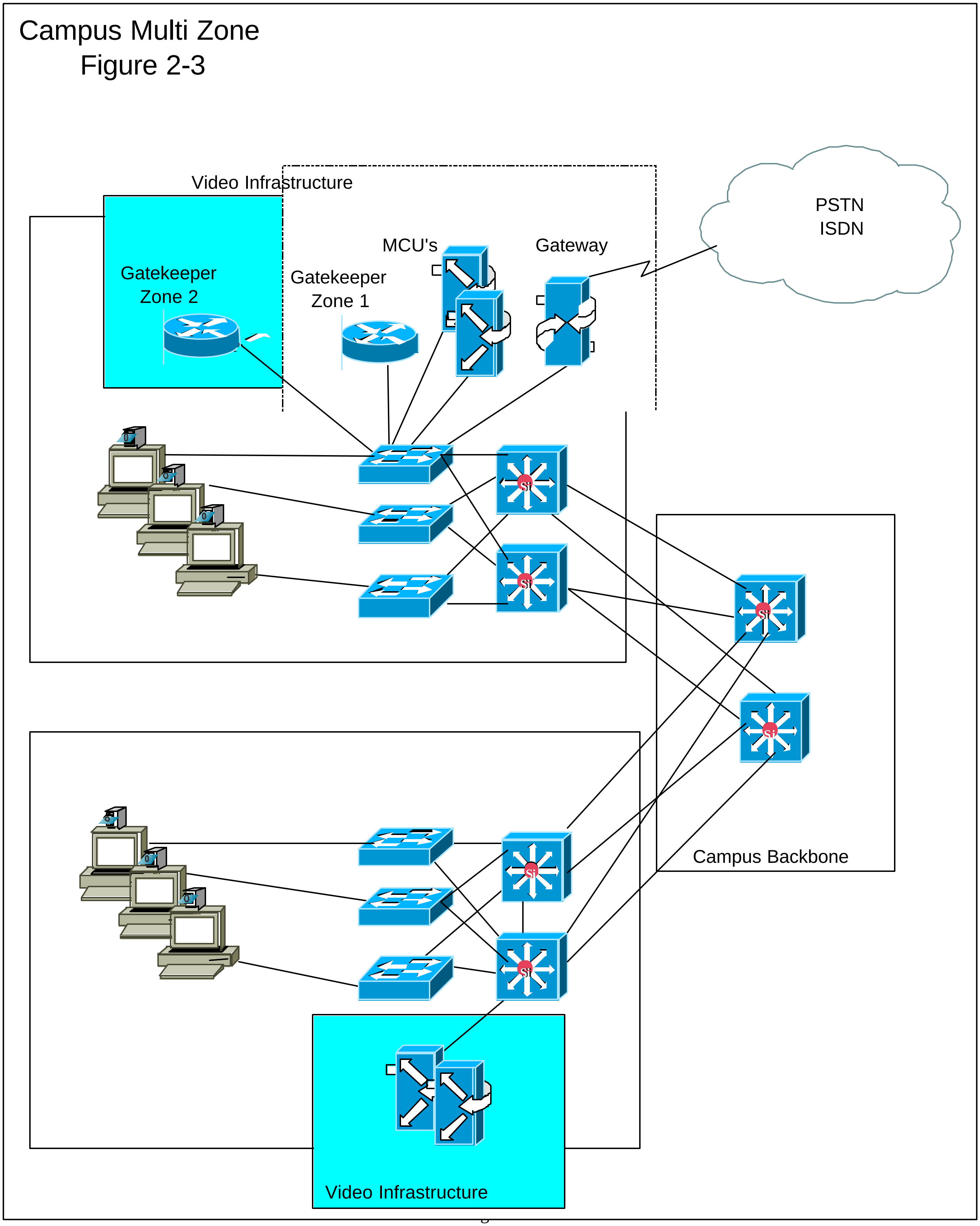
- A single gatekeeper supporting a single zone for H.323 video
- All H.323 video users registered with a single gatekeeper (see Chapter 8 for gatekeeper registration limits)
- Optional PSTN access available through IP/VC 352X gateway
- Optional Multipoint conferencing available through the IP/VC 3510 MCU
- Zone bandwidth managed by the configured gatekeeper
- All gateway and MCU services registered and managed by a single gatekeeper
- Call routing between endpoints using fully qualified E.164 addresses or H323-ID

## Campus Multi zone:

Figure 2-3 illustrates a multi zone H.323 video network in a campus environment. This is the deployment that will be implemented most often in an enterprise campus network. Depending on business function administrators may choose to create zones for security reasons. Company executives may be registered in a single zone allowing administrators to limit access to those video terminals. Also as a video network grows a single zone may not be manageable based on the number of users, or the ability to manage network resources.

Note: Multiple zones can be configured on a single router. If multiple zones are configured on a single router and MCUs and or gateways are registered with the zones, hopoff statements must be added for each service prefix. See Inter zone call routing using hopoffs on page 63 for more information.

**Figure 2-3**


Campus Multi Zone
Figure 2-3
Video Infrastructure
Gatekeeper
Zone 2
MCU's
Gatekeeper
Zone 1
Gateway
PSTN
ISDN
Campus Backbone
Video Infrastructure

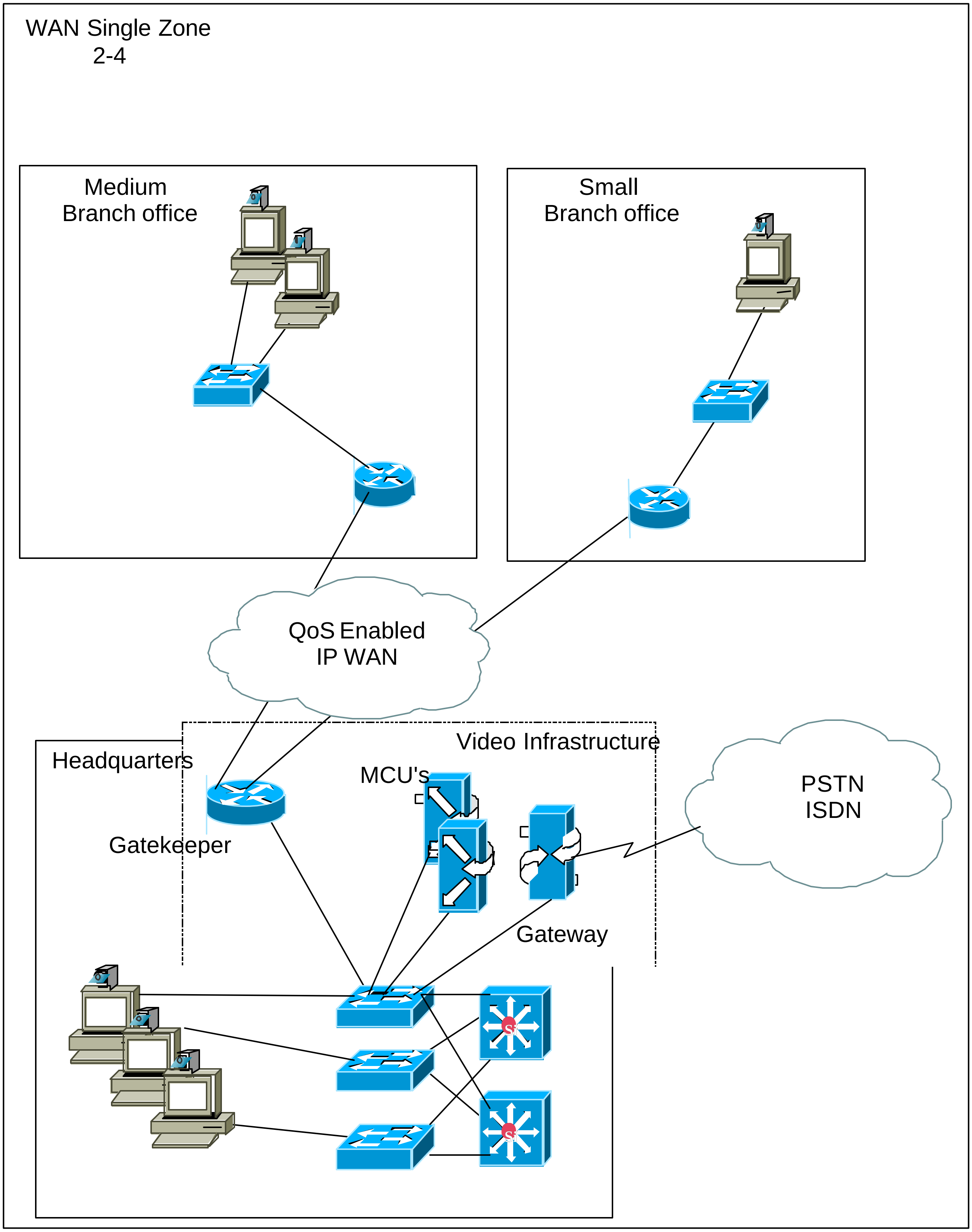
The Campus multi zone deployment model has the following design characteristics:

- Multiple gatekeepers supporting multiple zones for H.323 video
- H.323 endpoints register with one of the multiple gatekeepers (see Chapter 8 for gatekeeper registration limits)
- Bandwidth management for each zone and between zones controlled by configured gatekeepers
- Optional PSTN access available through IP/VC 352X gateway
- Gateway and MCU services registered and managed across multiple gatekeepers
- Gateway and MCU services may distributed throughout the campus
- H.323 users and services segmented for security, bandwidth control, and resource allocation
- Intra-zone and Inter zone call routing using fully qualified E.164 address or H323-ID

## WAN Single Zone:

Figure 2-4 illustrates a single zone H.323 video network in a WAN environment. This deployment model is used when remote sites have a small number of video endpoints, usually no more than one or two at each remote site. (Note: the number of video terminals described above is based on a T1 WAN link.) From a management or economic standpoint it may not make sense to create a zone at each remote site for one or two video terminals. Call admission control (CAC) across the WAN is not usually an issue with one or two video terminals in each remote site. It is only an issue when the number of remote endpoints exceeds the provisioned video bandwidth amounts. Quality of service in the absence of a the Cisco proxy will also need to be implemented on the WAN ports using priority queuing on traffic classification, or by creating an ACL for each video terminal at the remote site that will direct the video streams to the appropriate PQ.

**Figure 2-4**


WAN Single Zone
2-4
Medium
Branch office
Small
Branch office
QoS Enabled
IP WAN
Headquarters
Video Infrastructure
MCU's
Gatekeeper
Gateway
PSTN
ISDN

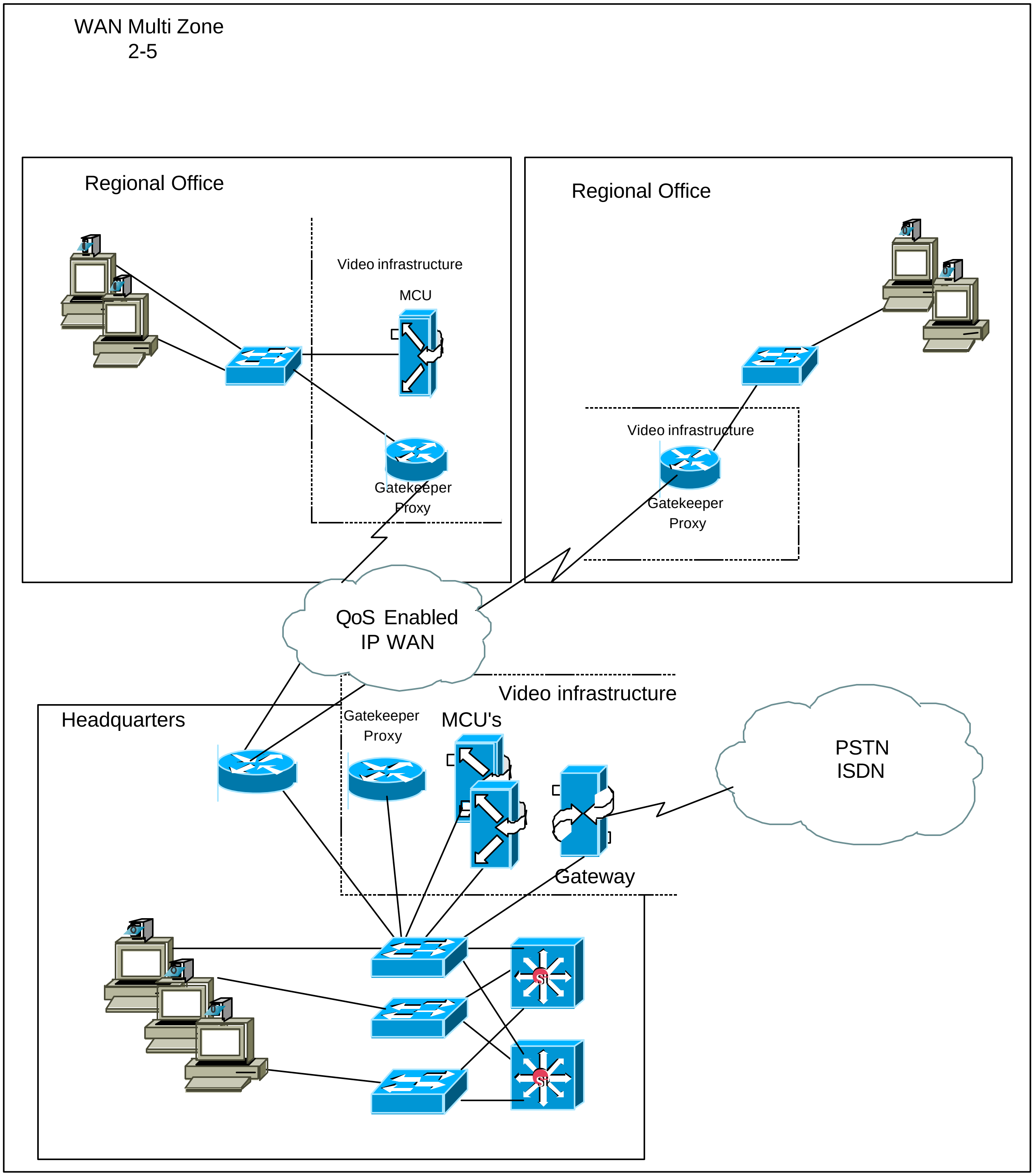
The WAN single zone deployment model has the following design characteristics:

- A single gatekeeper supporting a single zone for H.323 video
- All H.323 video users registered with a single gatekeeper (see Chapter 8 for gatekeeper registration limits)
- Optional PSTN access available through IP/VC 352X gateway
- Optional Mult ipoint conferencing available through the IP/VC 3510 MCU
- H.323 video bandwidth managed by a single gatekeeper
- All gateway and MCU services registered and managed by a single gatekeeper
- WAN QoS: traffic classification and priority queuing, or ACL entries with priority queuing
- Call routing between endpoints using fully qualified E.164 addresses or H323-ID

# WAN Multi Zone:

Figure 2-5 illustrates a multi zone H.323 network in a WAN environment. This deployment model will be seen in large enterprise, government and educational networks. Quality of service can be implemented using the proxy and priority queuing (PQ) in Cisco IOS software, or by using traffic classification by the video terminals or layer three switches in conjunction with PQ on the WAN ports of the routers. Creating multiple zones in a WAN environment allows administrators to manage network resources, and assure video quality across low speed WAN links. Call admission control (CAC) is very important in a large WAN environment. By creating multiple zones, bandwidth can be managed by the gatekeepers in the network. . CAC is used to manage the total amount of H.323 video bandwidth allowed across a particular network link. For example, you could limit the total H.323 video bandwidth allowed across a T-1 WAN link to 768k. The gatekeeper will then reject any call request that exceeds the 768k limits across the WAN.

## Figure 2-5


WAN Multi Zone
2-5
Regional Office
Video infrastructure
MCU
Gatekeeper
Proxy
Regional Office
Video infrastructure
Gatekeeper
Proxy
QoS Enabled
IP WAN
Video infrastructure
Headquarters
Gatekeeper
Proxy
MCU's
PSTN
ISDN
Gateway

The WAN multi zone deployment model has the following design characteristics:

- Multiple gatekeepers supporting multiple zones for H.323 video
- H.323 endpoints and services register with the assigned gatekeeper (usually at the local site)
- Optional PSTN access available through IP/VC 352X
- Bandwidth management available in each zone and across the WAN, using the gatekeeper at each site
- Distributed services are available at larger branch sites to conserve bandwidth
- Inter zone and Intra zone call routing using fully qualified E.164 addresses or H323-ID
- Proxy is enabled at each site with PQ on the WAN, or PQ based on traffic classification is implemented on WAN ports.

# Chapter 3:

# Campus Infrastructure:

This chapter provides guidelines for H.323 video deployed on a campus network. There are two basic H.323 video designs that will be discussed in the campus and WAN. There is a single zone design and a multi zone design. This section will cover single and multi zone design in a campus network.

This chapter contains the following sections:

- Overview
- Campus Infrastructure
- Campus Single Zone
- Campus Multi Zone
- Quality of Service

## Overview:

Building an H.323 video network requires a well-designed network based on Cisco multi-protocol routers, and Catalyst multi-layer LAN switches. This will ensure video quality and future network scalability. Below both single zone and multi-zone campus networks are discussed.

## Network Infrastructure:

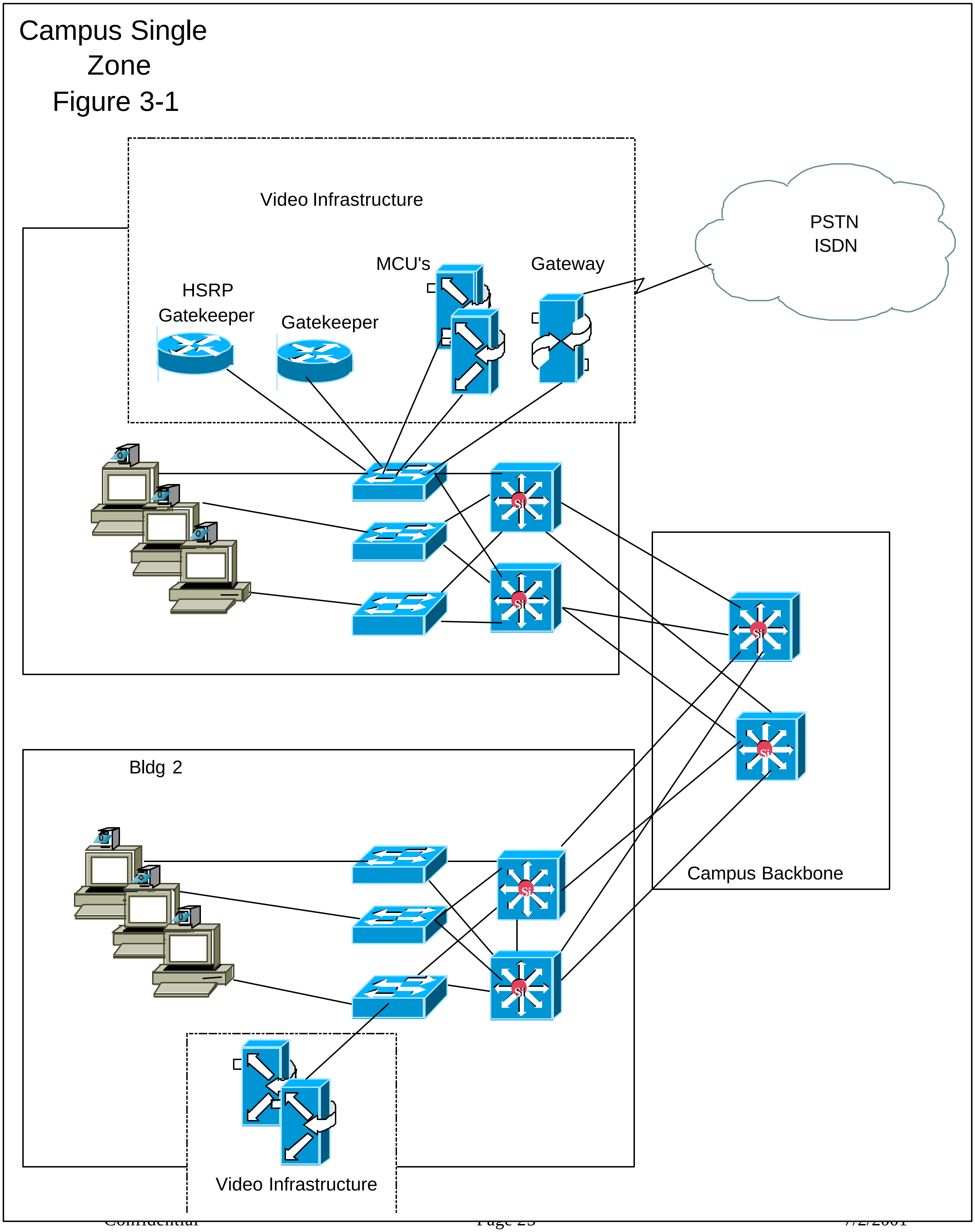
Building an end-to-end H.323 video network requires an infrastructure based on layer 2 and layer 3 switches and routers. It is important that all H.323 video endpoints, gateways, and MCUs are connected to a dedicated 10/100 switched-Ethernet port. 100Mbps full duplex should always be used for Cisco gatekeeper connectivity, this will ensure adequate bandwidth on all router platforms. Some endpoints do not support 100 full duplex, older Polycom ViewStations and the IP/VC 3530 both support 10 Mbps half duplex only.

Note: There are known issues with some Catalyst switches and video endpoints negotiating half/full duplex. If the negotiation fails the endpoint will still function, but the system will experience video freezing every three to five seconds. It is a good idea to set all switch ports attached to H.323 video devices to 100 Mbps whenever possible, all video units also support 10 Mbps connections as well. The IP/VC 3530 and Polycom ViewStations support 10Mbps half duplex only.

## Campus Single Zone:

Figure 3-1 illustrates an H.323 single zone campus network:

**Figure 3-1**


Campus Single
Zone
Figure 3-1
Video Infrastructure
PSTN
ISDN
MCU's
Gateway
HSRP
Gatekeeper
Gatekeeper
Bldg 2
Campus Backbone
Video Infrastructure

Single zone campus networks are usually deployed in pilot deployments or in large campuses with a limited number of video terminals. The single zone campus deployment allows an administrator to deploy H.323 video on the campus while keeping management overhead to a minimum. There is only one gatekeeper to manage and the dial plan is very simple with no inter zone call routing. It is important to remember that multi zone dial plans should be considered when deploying a single zone model in the event that the network will ultimately scale to more diverse requirements. If a dial plan is deployed that will not scale to a multi zone model, the entire dial plan may have to be changed if the H.323 network expands to multiple zones.

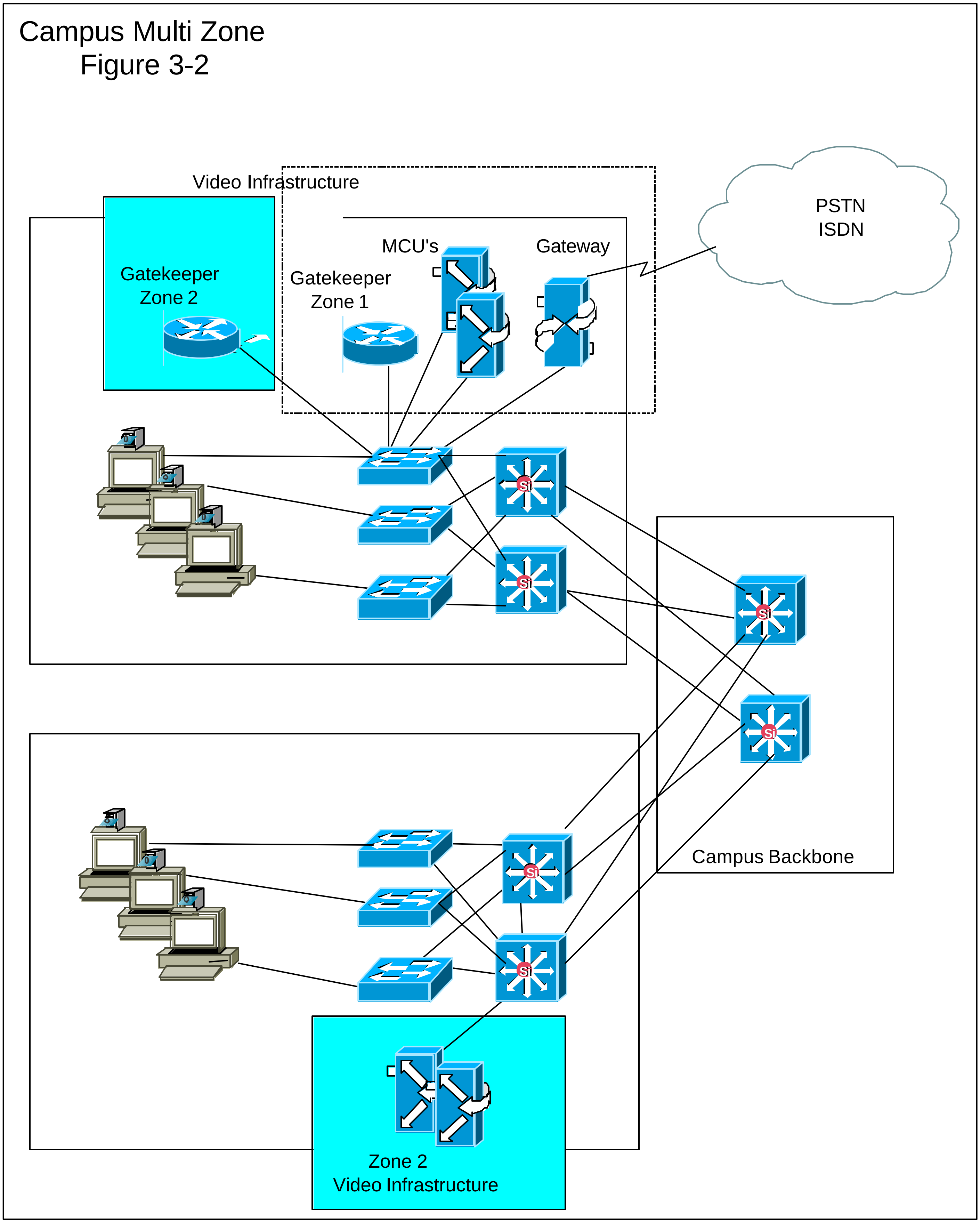
What constitutes a Campus Single Zone model?

- Campus environment
- Pilot environments
- Small number of video endpoints
- No bandwidth limitations

## Campus Multi Zone:

Figure 3-2 illustrates an H.323 Multi zone campus network:

## Figure 3-2


Campus Multi Zone
Figure 3-2
Video Infrastructure
Gatekeeper
Zone 2
MCU's
Gateway
Gatekeeper
Zone 1
PSTN
ISDN
Campus Backbone
Zone 2
Video Infrastructure

Multi zone campus networks will be common in large campus environments. Creating multiple zones allows administrators to segment user groups for security, better management of the H.323 video network, and limit bandwidth in and between zones. For example: some administrators may want the executive staff to have their own zone containing gateway and MCU resources that are only available to the executives. In campuses with a large number of video terminals it is important to control the amount of video bandwidth on the network. With a single zone bandwidth management is very limited. Creating multiple logical zones on the campus allows an administrator to limit bandwidth inside and between zones.

Physical placement of gatekeepers, MCUs, and gateways will depend on customer preference and network configuration. Some sites will locate all of the gatekeepers, MCUs, and gateways in a single data center, while others may decide to distribute the equipment through out the campus.

What constitutes a Campus Multi zone model?

- Campus environment
- Large numbers of video terminals
- Need to segment users into separate video "domains"
- Need to restrict access to some users

Note: Multiple zones can be configured on a single router. If multiple zones are configured on a single router, hopoff commands will need to be added for every service prefix registered. If hopoffs are not added inter "local" zone calls to MCUs will not work.

## Quality of Service

In a converged environment, voice, video and data traffic types travel over a single transport infrastructure. Yet all traffic types are treated equally. Data is bursty, loss tolerant, and delay in-sensitive. Video, on the other hand is bursty, has very little tolerance to loss, and is latency sensitive. The challenge is providing the required level of service for these traffic types.

Running both video and data on a common network requires the proper QoS tools to ensure that the delay and loss parameters of video traffic are satisfied in the face of unpredictable data flows. Some of these tools may be available as a feature in some video terminals (Polycom, VCON, and PictureTel), switches and routers.

## Traffic Classification Types

The goal of preserving video quality on a data network is first addressed by classifying video traffic as high priority, and then allowing it to travel through the network before lower priority traffic. Data traffic can be classified at a lower priority without adversely affecting its performance because of its characteristics as provided by the Transfer Control Protocol (TCP). Flow control and error correction are handled by the TCP protocol. Classification can be done at Layer 3 as follows

- At Layer 2 using the 3 bits in the 802.1Qp field (referred to as class of service CoS), which is part of the 802.1Q tag

- At layer 3 using the 3 bits of differentiated services code point (DSCP) field in the type of service (ToS) byte of the IP header

Classification is the first step towards achieving quality of service. Ideally, this step should be done as close to the source as possible. However, setting this field can also be accomplished within a router such as the Cisco MCM.

## Trust Boundaries

The concept of trust is an important and integral one to deploying QoS. Once the end devices have set CoS values, the switch has the option of trusting them or not. If the switch trusts the values, it does not need to do any reclassification; if it does not trust the values, then it must perform reclassification for appropriate QoS.

The notion of trusting or not forms the basis for the trust boundary. Ideally, classification should be done as close to the source as possible. If the end device is capable of performing this function, then the trust boundary for the network is at the access layer in the wiring closet. If the device is not capable of performing this function, or the wiring closet switch does not trust the classification done by the end device, the trust boundary should shift. How this shift happens depends on the capabilities of the switch in the wiring closet. If the switch can reclassify the packets, then the trust boundary remains in the wiring closet. If the switch cannot perform this function, then the task falls to other devices in the network going towards the backbone. In this case the rule of thumb is to perform reclassification at the distribution layer. This means that the trust boundary has shifted to the distribution layer. It is more than likely that there is a high-end switch in the distribution layer with features to support this function. If possible, try to avoid performing this function in the core of the network.

In summary, try to maintain the trust boundary in the wiring closet. If necessary, move it down to the distribution layer on a case-by-case basis, but avoid moving it down to the core of the network. This advice conforms to the general guidelines to keep the trust boundary as close to the source as possible.

Note:

This discussion assumes a three-tier network model, which has proven to be a scalable architecture. If the network is small, and the logical functions of the distribution layer and core layer happen to be in the same device, then the trust boundary can reside in the core layer if it has to move from the wiring closet. For more detailed configuration information refer to the AVVID QoS design guide. http://wwwin.cisco.com/ent/voice/sales/design_guides.shtml.

Table 3-1 shows support for traffic classification on each switch platform.

## Table 3-1

| **Platform** | **Ability to Trust** | **Reclassify CoS** | **Reclassify ToS** | **Congestion Avoidance (WRED** | **Priority Queues** | **Multiple Queues** | **Congestion Management (WRR)** | **Policing** |
|---|---|---|---|---|---|---|---|---|
| ***Catalyst 6000*** | ***Yes*** | ***Yes*** | ***Yes*** | ***Yes*** | ***Yes*** | ***Yes*** | ***Yes*** | ***Yes*** |
| ***Catalyst 5000*** | ***No*** | ***Yes*** | ***Yes1*** | ***Yes*** | ***No*** |  | ***No*** | ***No*** |
| ***Catalyst 4000*** | ***No*** | ***Yes*** | ***No*** | ***No*** | ***No*** | ***Yes*** | ***No*** | ***No*** |
| ***Catalyst 3500*** | ***Yes*** | ***Yes*** | ***No*** | ***No*** | ***Yes*** | ***Yes*** | ***No2*** | ***No*** |

**1.** With additional configuration
**2.** Round robin only

Note:
Currently the only Cisco LAN switches that support a minimum of two queues and that can guarantee video quality are the Catalyst 8500, Catalyst 6XXX family, Catalyst 4XXX family, Catalyst 3500XL, and Catalyst 2900XL.

Recommendations for QoS deployment:

- Create trust boundary at the network edge in the wiring closet.  Make ports trusted on the wiring closet switch where video terminals with the ability to set IP Precedence reside.

- Reclassify ToS at the edge if devices cannot be trusted.

- Shrink the trust boundary to the distribution layer and reclassify ToS there if reclassification is not possible at the edge.

- Use priority queue for delay-sensitive video traffic.

# Chapter 4:

# WAN Infrastructure:

This chapter provides guidelines for H.323 video deployed across an IP WAN. There are two basic H.323 video designs that will be discussed in the campus and WAN. There is a single zone design and a multi zone design. This section will cover single and multi zone design in an IP WAN

This chapter contains the following sections:

- Overview
- WAN Single Zone
- WAN Multi Zone

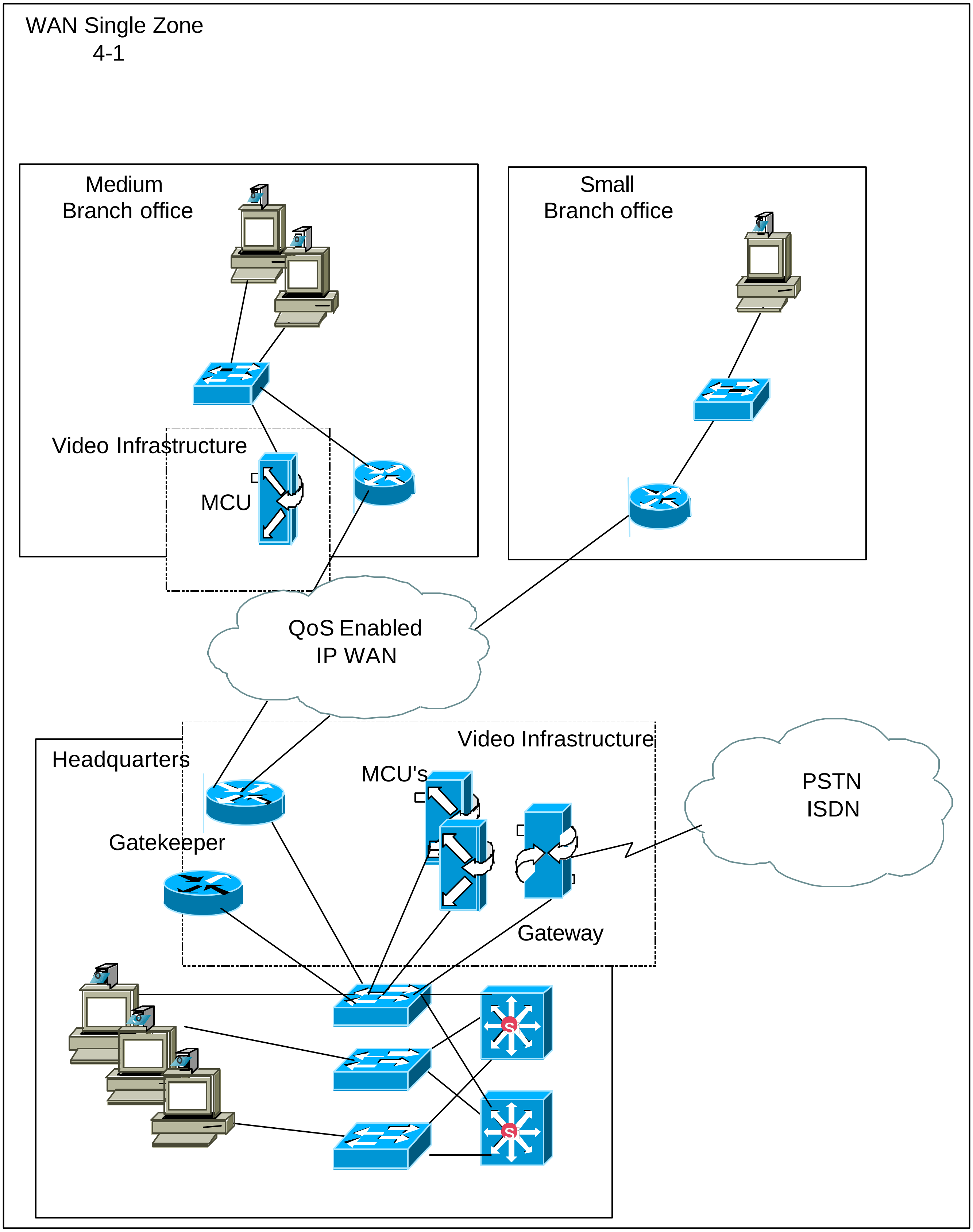
## Overview:

Building an H.323 video network requires a well-designed network based on Cisco multi-protocol routers, and Catalyst multi-layer LAN switches. This will ensure video quality and future network scalability. Below both single zone and multi-zone campus networks are discussed.

## WAN Single Zone:

Figure 4-1 illustrates an H.323 single zone WAN network:

## Figure 4-1


WAN Single Zone
4-1
Medium
Branch office
Video Infrastructure
MCU
Small
Branch office
QoS Enabled
IP WAN
Headquarters
Video Infrastructure
MCU's
Gatekeeper
Gateway
PSTN
ISDN

## WAN Single Zone Considerations:

What constitutes a WAN Single Zone Model?

- WAN Environment
- Less than three video terminals at remote sites

Single zone WAN deployments will be found in environments with remote sites containing one or two videoconferencing terminals at remote sites (this is based on a T1 WAN link). Configuring a gatekeeper and zone for a remote site with one or two video terminals is recommended but not necessary. Due to the limited number of endpoints and traffic classification options, QoS and CAC can be achieved by following two basic rules.

1. The total data rate of the video terminals + 20% should not exceed 33% of the WAN link capacity.

2. The Priority Queue must be provisioned for the maximum data rate of the video terminals + 20%. For example: A site has a link capacity of 1.544 Meg, and contains two video terminals that support a maximum data rate of 256k each. The maximum data rate of the two video terminals is 512k + 20% = 614k. Provisioning the PQ for 614k allows both video terminals to be in a call across the WAN at the same time, without the possibility of over running the PQ. In our example, if we add a third video terminal we would need to add a gatekeeper and create a zone to provide call admission control (CAC).

In a single zone WAN environment there are a few rules that need to be followed to ensure success. The five key elements are listed below. Figure 4-2 illustrates the three options for traffic classification.

- **Traffic Classification**

  Traffic Classification can be done at one of three places:
  1. Video endpoint (Polycom, VCON, & PictureTel) IP Precedence 4 only
  2. Switch port (layer 3 switch required) IP Precedence 4 \DSCP AF41
  3. Router (ACL entry) IP Precedence 4\DSCP AF41

- **Call Admission Control (CAC)**

  Remote sites do not have a gatekeeper to enforce CAC, so the Provisioning of the PQ, and the number of video terminals at each site will be the only CAC mechanism. The number of video terminals, times the maximum call data rate, must not exceed the capacity of the PQ. For this reason it is recommended that remote sites with more than two video terminals have their own gatekeeper\zone.

- **Provisioning**

  WAN queues must be provisioned for the number of users at remote sites, times the maximum data rate allowed on each video terminal, plus 20%. The PQ must be provisioned to handle this data rate or the PQ has the potential of being oversubscribed. Data rates should be calculated as follows: Data Rate + 20%, this will allow for IP and transport overhead. See Chapter 5 WAN QoS for more information.

- **Priority Queuing on the WAN**

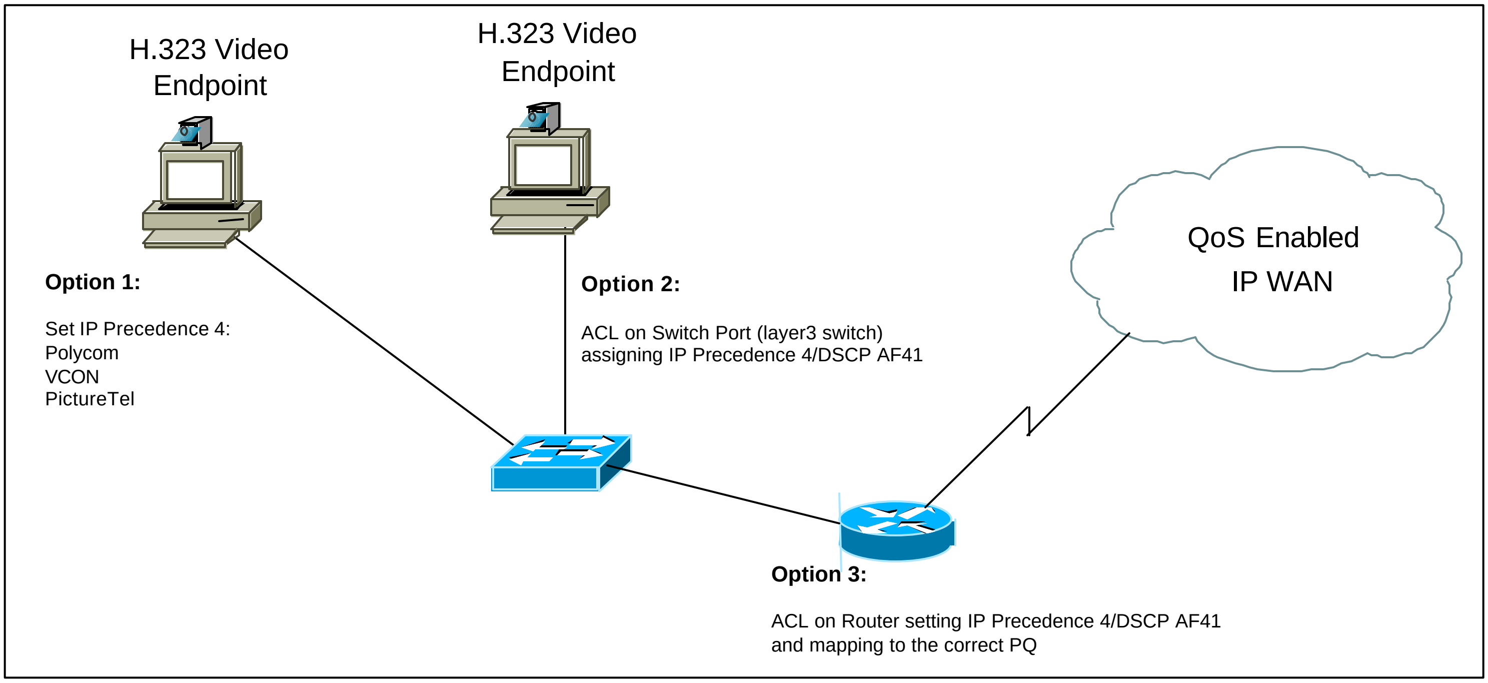
  WAN ports on routers will be configured with multiple queues. Videoconferencing will go into a PQ that services IP Precedence 4\DSCP AF41. Class based weighted fair queuing (CBWFQ) is not recommended for interactive video.

- **Entrance Criteria**

In the single zone WAN model ACLs should be used to access configured priority queues (PQ) at remote sites. This ensures that only traffic from the video terminals has access to the configure PQ. The limited number of video terminals at remote sites allows ACL entries to be an option.

Central sites that have video terminals capable of setting IP Precedence, or layer 3 switches, should set the entrance criteria for the PQ to any packets with IP Precedence set to 4 or DSCP AF41. This method is not as secure as the ACL option, but will work properly if the trust boundaries are configured correctly. This method can also be used at remote sites if ACLs are not acceptable.

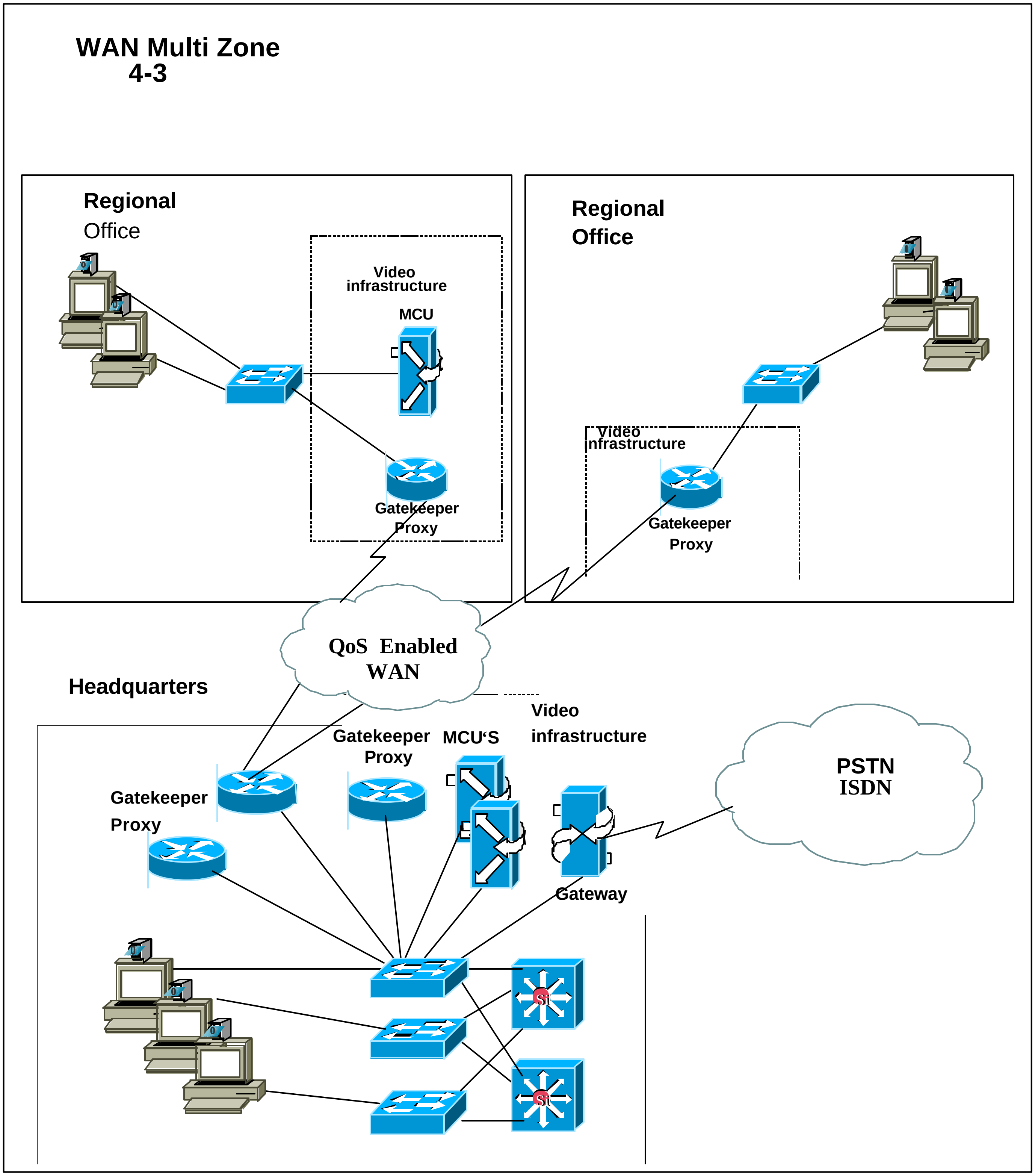
## Figure 4-2


H.323 Video Endpoint
H.323 Video Endpoint
QoS Enabled IP WAN
Option 1:
Set IP Precedence 4:
Polycom
VCON
PictureTel
Option 2:
ACL on Switch Port (layer3 switch) assigning IP Precedence 4/DSCP AF41
Option 3:
ACL on Router setting IP Precedence 4/DSCP AF41 and mapping to the correct PQ

## WAN Multi Zone:

Figure 4-3 illustrates a Multi Zone WAN Network:

## Figure 4-3



What constitutes a WAN Multi Zone Model?

- WAN Environment
- More than three video terminals at a remote site

Note: The above three video terminals is based on T1 connectivity to a remote site. If the PQ at the remote site is provisioned for two 384k calls adding a third terminal would require a gatekeeper to administer CAC or the ability to provision the PQ for a third 384k call. Since a site connected with a T1 should not be provisioned for three 384k calls it is recommended that a gatekeeper zone be configured to support the remote site.

Multi zone WAN deployments will be found in large enterprise and state based distance-learning networks. Remote sites will contain three or more video terminals that will be managed by a local gatekeeper. This allows the local gatekeeper to manage bandwidth in the local zone and across the WAN between zones. It is only possible to manage bandwidth in a hub and spoke environment today. Intermediate gatekeepers are not aware of a call that is passing through its zone. Only the originating zone gatekeeper and terminating zone gatekeeper will be aware of the active call.

Figure 4-3 shows each remote site running the Gatekeeper/Proxy on the WAN router, and dedicated routers running HSRP for Gatekeeper/Proxy at the central site. There are two factors that will come into play when deciding on a dedicated router for the Gatekeeper/Proxy or a shared router. The first consideration is whether the customer feels comfortable running the required router code for Gatekeeper/Proxy support. The second consideration is the number of registered endpoints and simultaneous calls being processed. It is recommended that a dedicated router be used if there are more than 20 registered endpoints at a given site.

In a multi zone WAN environment the same rules apply that were outlined in the single zone WAN deployment. The biggest difference is the ability to control bandwidth and an added classification point. The five key elements are outlined below. Figure 4-4 illustrates classification options for a multi zone WAN model.

- **Traffic Classification**

  Traffic Classification can be done at one of four places:
  1. Video endpoint (Polycom, VCON, & PictureTel) IP Precedence 4 only (recommended)
  2. Proxy classification IP Precedence 4 or RSVP (recommended for traffic reclassification)
  3. Switch port (layer 3 switch required) IP Precedence 4 \DSCP AF41 (this is recommended only for room based systems)
  4. Router (ACL entry) IP Precedence 4\DSCP AF41 (most likely won't be used due to the larger number of video terminals at each site)

- **Bandwidth Control\Call Admission Control (CAC)**

  Now that each remote site contains a gatekeeper/zone bandwidth control between zones is possible. By configuring the "Remote" bandwidth in each gatekeeper, administrators can limit the amount of available bandwidth for calls to and from the WAN.

- **Provisioning**

  WAN queues will be provisioned based on the bandwidth limits set in the gatekeeper, remember not to provision more than 33%of the link capacity to video applications. Engineering recommends that voice and video traffic take no more than 33% of link capacity.

- **Priority Queuing on the WAN**

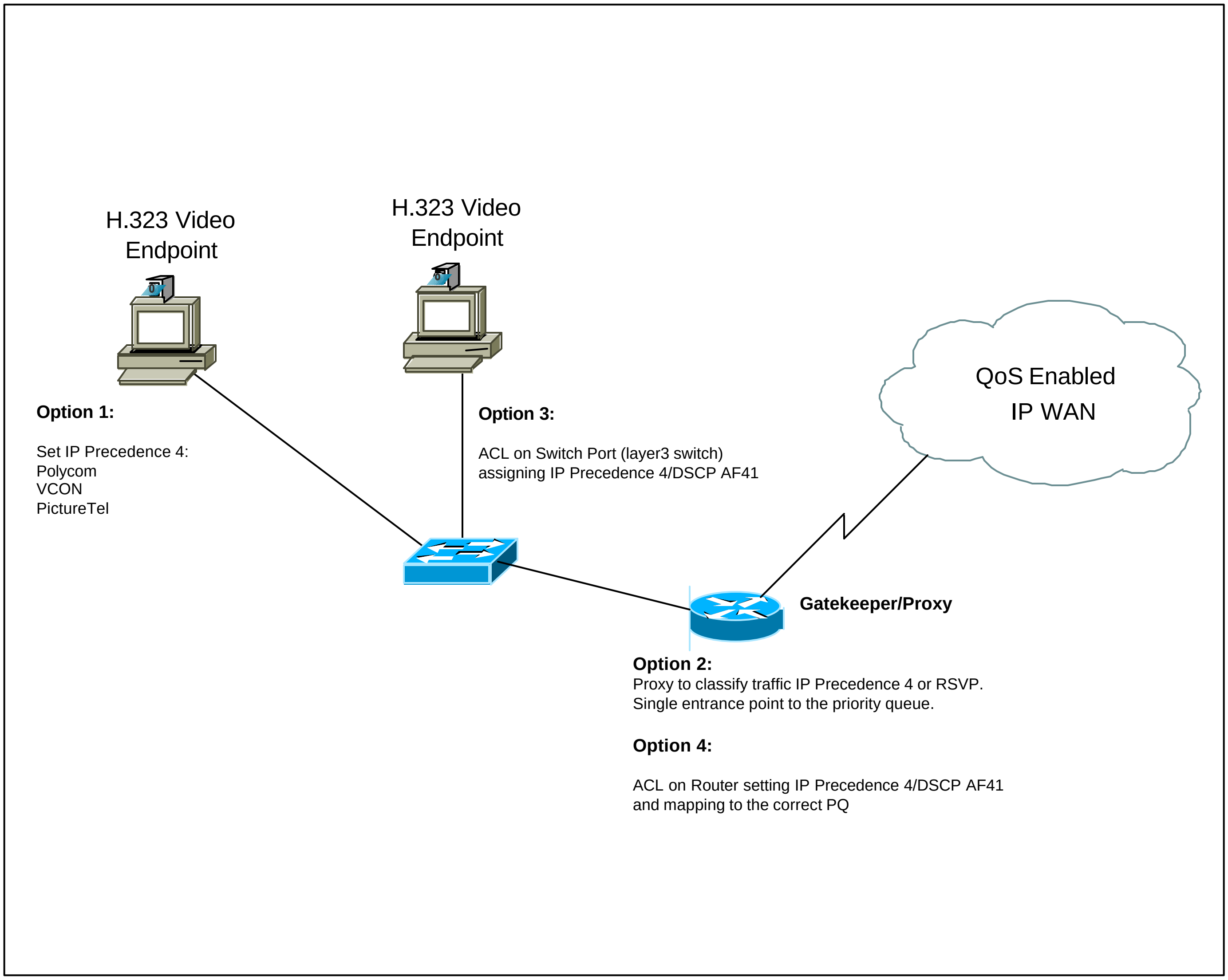
  WAN ports on routers will be configured with multiple queues. Videoconferencing will go into a PQ that services the Proxy only, or streams marked with IP Precedence 4 or DSCP AF41.

- **Entrance Criteria**

  Using the Proxy allows administrators to limit access to the priority queue (PQ). By configuring an ACL on the WAN router only packets received from the Proxy will have access to the configured PQ. This will ensure that an unauthorized user installing a video terminal on their desk, and dialing using an IP address, do not get access to the PQ potentially oversubscribing it.

  If the Proxy is not used the entrance criteria for the PQ should be any packets with IP Precedence set to 4 or DSCP AF41.

# Figure 4-4



**Option 1:**

Set IP Precedence 4:
Polycom
VCON
PictureTel

**Option 3:**

ACL on Switch Port (layer3 switch)
assigning IP Precedence 4/DSCP AF41

**Option 2:**
Proxy to classify traffic IP Precedence 4 or RSVP.
Single entrance point to the priority queue.

**Option 4:**

ACL on Router setting IP Precedence 4/DSCP AF41
and mapping to the correct PQ

# Chapter 5:

# WAN QoS

This chapter addresses the quality of service (QoS) requirements for implementations of H.323 videoconferencing solutions over the enterprise WAN. By applying the prerequisite tools, you can achieve excellent video, voice and data transmission over an IP WAN, irrespective of media and even low data rates and also accommodate an enterprise's data requirements.

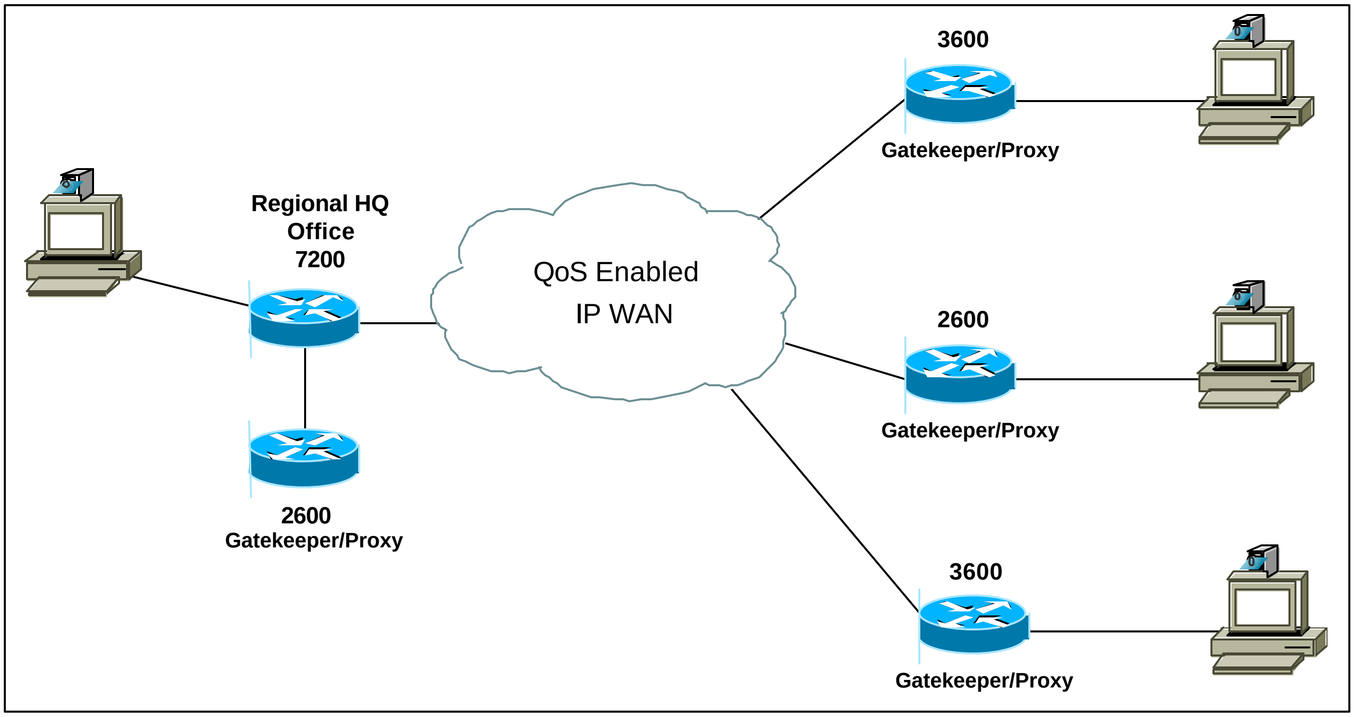
This chapter includes the following sections:

- WAN QoS Model
- Capacity Planning
- QoS Tools
- Best Practices Recommendations
- Call Admission Control

## WAN QoS Model

The enterprise WAN model is shown in Figure 5-1

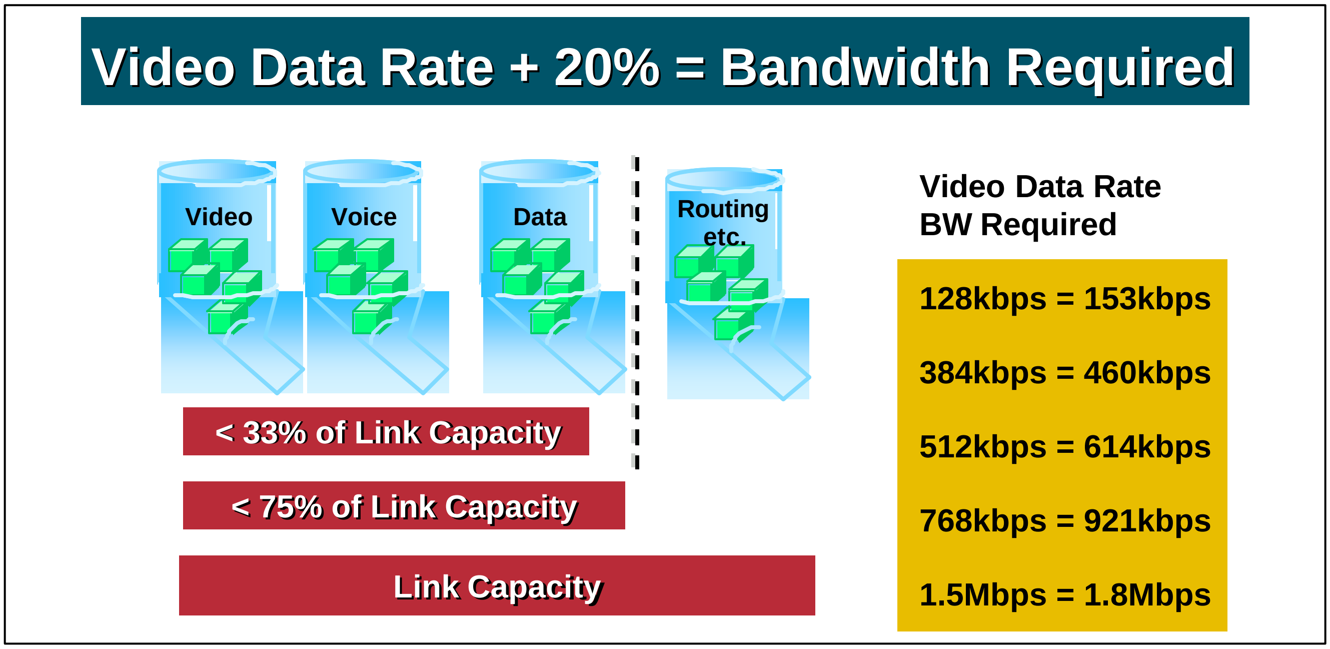
### Figure 5-1



## Capacity Planning:

Before video can be placed on a network, it is necessary to ensure that adequate bandwidth exists for all required applications. To begin, the minimum bandwidth requirements for each major application (for example, voice, video, and data) should be summed. This sum then represents the minimum bandwidth requirement for any given link, and it should consume no more than 75% of the total bandwidth available on that link. This 75% rule assumes that some bandwidth is required for overhead traffic such as routing and layer 2 keepalives, as well as additional applications such as e-mail and HTTP traffic. Figure 5-2 illustrates capacity planning on a converged network.

## Figure 5-2



Video Data Rate + 20% = Bandwidth Required

Video Data Rate
BW Required

128kbps = 153kbps

384kbps = 460kbps

512kbps = 614kbps

768kbps = 921kbps

1.5Mbps = 1.8Mbps

## QoS Tools:

This section discusses the tools used to implement QoS for H.323 videoconferencing over an enterprise WAN. These tools include traffic classification, proxy usage, and prioritization. This section concludes with a summary of best practices for each of the applicable data link protocols.

## Traffic Classification:

Before traffic can be handled according to its unique requirements, it must be identified or labeled. There are numerous classification techniques for doing this. These include Layer 3 schemes such as IP Precedence or differentiated services code point (DSCP).

In many cases, traffic classification is done at the edge of the network by video terminal or Ethernet switch such as the Catalyst 6000. In these cases, the trust boundary is extended to the edge of the enterprise network and resides in the access or distribution layer. For a more detailed discussion of trust boundaries, see the "Trust Boundaries" section on page 28.

In some cases, however the ability to classify and define a trust boundary at the edge of the network might not exist, such as in a branch with Ethernet switches and video endpoints that can't classify traffic. In this situation, the trust boundary and classification can be achieved on the route itself. This can be done through ACL entries for small sites without a gatekeeper, or by using the Proxy in larger branch sites that contain a gatekeeper.

## Proxy Usage:

In the Multi Zone WAN model it is recommended that the proxy be used when ever possible. The proxy allows the classification or reclassification of video streams with IP Precedence or RSVP. The proxy also allows a single access point to the priority queue keeping unauthorized video streams from oversubscribing the priority queue. Video terminals must be registered with the gatekeeper to obtain access to the proxy. The gatekeeper will be configured for a maximum video bandwidth allowed outside its local zone. This maximum bandwidth should match the amount of bandwidth provision on the priority queue to ensure proper queuing functionality.

## Traffic Prioritization:

In choosing from among the many available prioritization schemes, the major factors to consider include the type of traffic being put on the network and the wide area media being traversed. For multi service traffic over an IP WAN, Cisco recommends low latency queuing for low speed links. This allows up to 64 traffic classes with the ability to use multiple queues for different traffic types. For example, priority queuing behavior for videoconferencing and voice, a minimum bandwidth for SNA data and market data feeds, and weighted fair queuing to other types of traffic.

Figure 5-3 shows this prioritization scheme as follows:

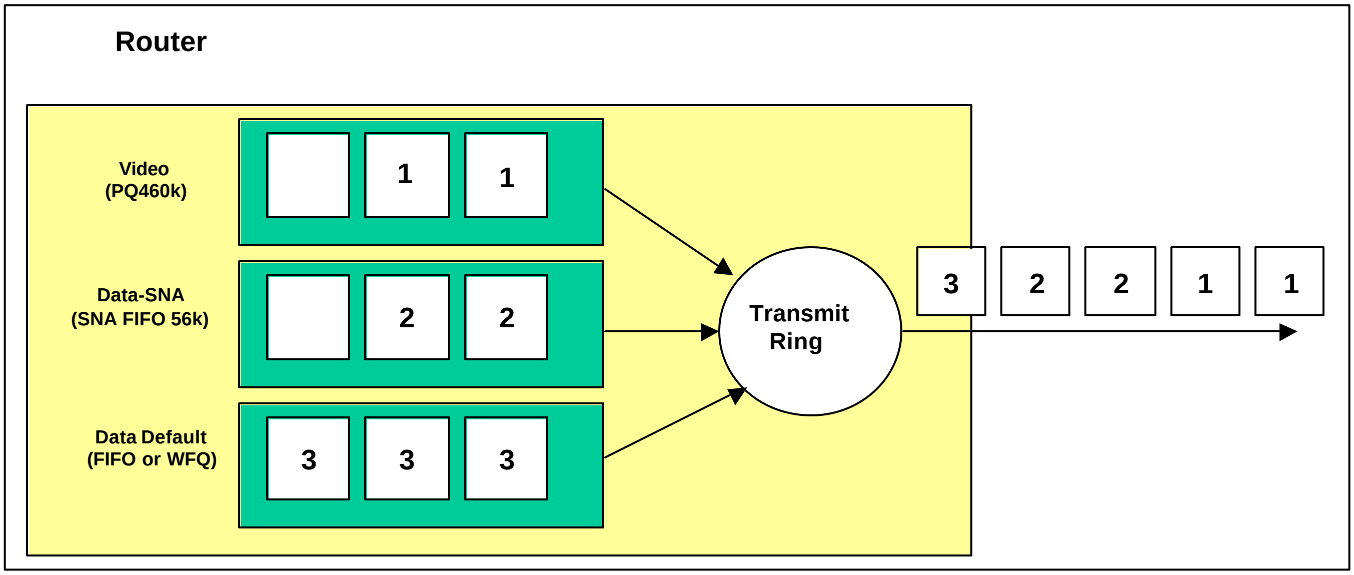
- Video is placed into a queue with priority queuing capabilities and is allocated a bandwidth of 460kbps. The entrance criterion to this queue could be any video stream received from a specific IP address of a proxy, or any traffic with IP Precedence set to 4. Traffic in excess of 460k would be dropped if the interface becomes congested. Therefore, an admission control mechanism (such as gatekeeper bandwidth limits) must be used to ensure that this value is not exceeded.

- SNA traffic is placed into a queue that has a specified bandwidth of 56k. Queuing operation within this class is first-in-first-out (FIFO) with a maximum allocated bandwidth of 56kbps. Traffic in this class that exceeds 56 kbps is placed in the default queue. The entrance criterion to this queue could be TCP port numbers, Layer 3 address, IP Precedence or DSCP.

- All remaining traffic can be placed in a default queue. If a bandwidth were specified, the queuing operation would be FIFO. Alternatively, by specifying the keyword **fair,** the operation would be weighted fair queuing.

Figure 5-3 illustrates optimized queuing for videoconferencing of the WAN.

## Figure 5-3



The following points must be taken into account when configuring low latency queuing.

- The minimum system software for leased lines and ATM is Cisco IOS Release 12.0(7) T.

- The minimum system software for Frame Relay is Cisco IOS Release 12.1(2) T.

Table 5-1 gives the minimum bandwidth requirements for video and data networks. Note these values are ***minimum***, and any network should be engineered with adequate capacity.

## Table 5-1

| Traffic Type | Leased Lines | Frame Relay | ATM | ATM/Frame Relay |
|---|---|---|---|---|
| Video + Data Max. Video Data Rates Up to 384kbps | 768 kbps | 768 kbps | 768 kbps | 768 kbps |
| Video + Data Max. Video Data Rates >384kbps | 1.544 Mbps | 1.544 Mbps | 1.544 Mbps | 1.544 Mbps |

## Best Practices Recommendations:

Table 5-2 shows the minimum recommended software release for enterprise video over the WAN and includes recommended parameters for QoS tools. The currently recommended IOS versions will change with future releases.

## Table 5-2

| Data Link Type | Minimum IOS | Classification | Prioritization | LFI | Traffic Shaping | cRTP |
|---|---|---|---|---|---|---|
| Serial Lines | 12.0(7)T | IP prec = 4, DSCP = AF41 for Video; other classes of traffic have a unique classification | LLQ with CBWFQ | N/A | N/A | N/A |
| Frame Relay | 12.1(2)T | IP prec = 4, DSCP = AF41 for Video; other classes of traffic have a unique classification | LLQ with CBWFQ | N/A | Yes | N/A |
| ATM | 12.0(7)T | IP prec = 4, DSCP = AF41 for Video; other classes of traffic have a unique classification | LLQ with CBWFQ | N/A | Yes | N/A |
| ATM/ Frame Relay | 12.1(2)T | IP prec = 4, DSCP = AF41 for Video; other classes of traffic have a unique classification | LLQ with CBWFQ | N/A | Yes | N/A |

Note:   cRTP is not recommended for use with IP videoconferencing.  Best practices for CRTP are listed below:

1.  Use cRTP only with low bit rate voice codec's such as G.729 used.  If G.711 is used is used as the audio codec for a voice or videoconference call the statistical throughput gains achieved with cRTP are not significant enough to merit it's use.

2.  Use cRTP only when Low Bit Rate Voice is a significant percentage of the offered load. In general this feature is only beneficial when low bit rate voice exceeds greater 30% of the offered load to a circuit.

3.  Be cognizant that cRTP can affect forwarding performance and it is recommended that CPU utilization be monitored when the feature is enabled.

## Call Admission Control:

Call Admission Control (CAC) or bandwidth control is required to ensure that the network resources are not oversubscribed.  Calls that exceed the specified bandwidth are rejected to ensure video quality.

There are only two schemes for providing CAC for video calls over the WAN:

- Limited number of video terminals: Limiting the number of video terminals for CAC is only necessary in the Single Zone WAN Model.  With the lack of a gatekeeper at remote sites, the only way to control the amount of bandwidth used for video across the WAN is to physically limit the number of video terminals at remote sites.  The Priority queue at each site must then be provisioned for the maximum possible data rate of all the video endpoints at any given site.  See page 33 for more information on this CAC scheme.

- Gatekeeper CAC: This is only available in the Multi Zone WAN Model.   The gatekeeper allows administrators to set bandwidth limits for inter zone, intra zone or on a per session basis.  This allows administrators the ability to set an inter zone or remote bandwidth limit, provision a priority queue for the same bandwidth, and ensure the integrity of that queue.  Note that today gatekeeper based CAC is limited to hub and spoke configurations.  See page 32 for more information on this CAC scheme

Note:  RSVP will allow end-to-end QoS over multi-tiered H.323 networks.  RSVP synchronization will be available in an upcoming release of the MCM to address this issue.

# Chapter 6:

# Dial Plan Architecture:

This section defines and explains the key elements in the design of a dial plan of an H.323 network. An H.323 video dial plan is a numbering scheme that allows H.323 video endpoints to dial other video endpoints or video services (MCU or Gateway). Each of these components will be discussed in a single zone and multi zone scenario.

This Chapter contains the following sections:

- Dial Plan Components
- Service Prefix Design
- Single Zone Dial Plan
- Zone Prefix Design
- Multi Zone Dial Plan

## Dial Plan Components:

A well-designed dial plan is a key component to a successful H.323 video network. A dial plan is one of the first things that need to be considered when designing an H.323 video network. Without a well thought out dial plan it will be impossible to scale the network. H.323 dial plans consist of four key elements, E.164 address, H323-ID, zones prefixes and service prefixes. Each of these items is defined below. Table 6.1 shows the components of a video and VoIP dial string as well as the correlation between the two.

**E.164 address:**

An E.164 address is a numeric identifier defined on each H.323 video endpoint, just as E.164 is used in the telephony world.

**H.323-ID:**

An H323-ID is an alphanumeric identifier defined on each H.323 video endpoint. An H323-ID may also be referred to as an alias, and can be used to dial an H.323 endpoint. Email addresses are often used as H323-IDs. H323-ID's can't be used to dial to the PSTN or to an IP/VC 3510 MCU.

**Zone Prefix:**

A zone prefix is a numeric prefix that identifies a zone. Zone prefixes are used for inter zone call routing, the same way an area code is used in the telephony world. Each zone in an H.323 network will have one unique zone prefix. Area codes are often used as zone prefixes in H.323 networks.

### Table 6-1

| **Video Dial String** | **Service Prefix** | **Zone Prefix** | **E.164 Address** | |
|---|---|---|---|---|
| **VoIP Dial String** | **Technology Prefix** | **Area Code** | **Local Exchange** | **Unit ID** |

## Service\Technology prefix:

| **Service Prefix** | Zone Prefix | E.164 Address |
|---|---|---|

A service prefix is a numeric prefix that is used in an H.323 dialing string for accessing a defined service on an MCU or gateway. The Cisco gatekeeper refers to Service Prefix as a Technology prefix, which is also used by H.323 voice gateways. In this document we will refer to these prefixes as a service prefix. Service prefixes are used on video gateways and MCUs to define parameter settings for that device. On an IP/VC 352X video gateway a service prefix defines the type of call being made (voice or video), and the data rate of the call. On an IPVC/3510 MCU service prefixes define the data rate of the call, number of participants, and picture format. When an MCU or video gateway registers with the gatekeeper it will register all defined service prefixes. When an H.323 endpoint uses a video gateway or MCU the dial string must start with the service prefix followed by the PSTN number being dialed (in the case of a Gateway call) or the conference ID being created or joined (in the case of an MCU call).

## Service Prefix Design:

Service prefixes are a very important part of the dial plan. Inter and Intra zone calls to an MCU or gateway will be routed using the service prefix. Service prefixes are configured in MCUs and gateways to define services and route calls. The single zone and multi zone models are very similar, but there is a minor difference. Both single zone and multi zone are discussed below. It is important to keep dial strings intuitive; with the models below dial strings are very similar to telephony dial strings. Dia l strings are reviewed in Chapter 7 Call Scenarios.

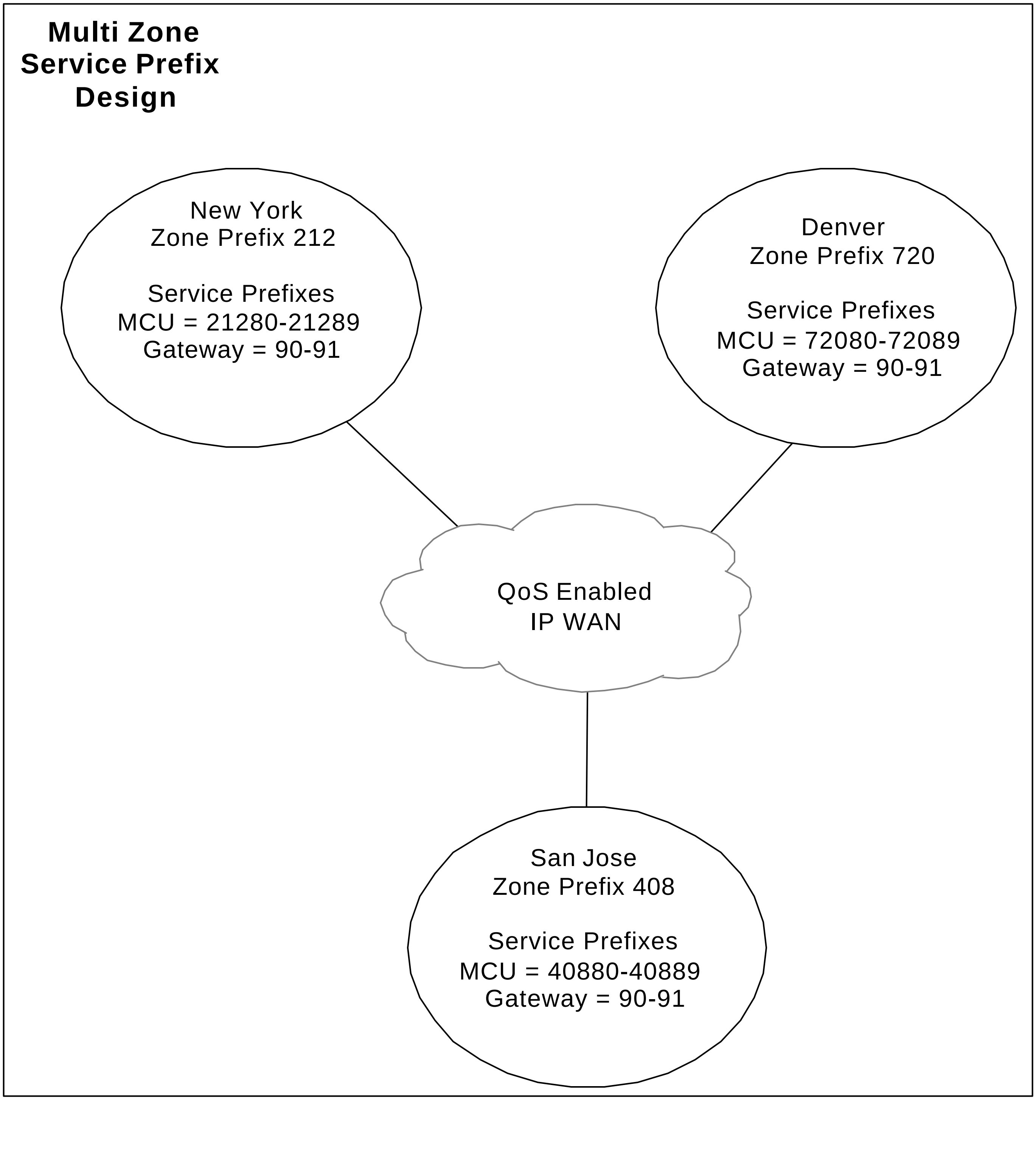
In a single zone network it is recommended that a block of numbers be reserved for service prefixes, say 8* for MCUs and 9* for gateways (the asterisks denote a wildcard, such as the digit “8” and “anything” following that. The * is not dialed by the user when placing a call). It is also recommended that the local area code be added to the service prefixes of MCUs, San Jose’s MCU might have a service prefix of 40880 = 384k. Gateway prefixes will remain 9*, this keeps dial strings consistent with the telephony world. This service prefix structure also allows an easy migration to a multi zone dial plan. E.164 addresses must not overlap with service prefixes. If an MCU registers with a service prefix of 40880* and a video terminal registers with 4088011212, all calls made to the video terminal will be routed to the MCU.

In a multi zone network, service prefixes need to routed between zones, and therefore requires all service prefixes to be unique across all zones. All calls routed to services Inter or Intra zone will be routed based on the service prefix. It is recommended that service prefix design in a multi zone network allow user dial strings to be consistent. To accomplish this there will be different approaches for service prefixes on gateways and MCUs. Service prefixes, E.164 addresses and zone prefixes must not overlap, or call routing issues will arise.

MCUs will need to be accessible from any H.323 endpoint on the network. This requires that all service prefixes in all zones be unique. In order to accomplish the unique service prefixes without reserving large blocks of numbers, it is recommended that MCU service prefixes be a combination of the zone prefix and a service number. This will allow all the service prefixes for MCUs to be consistent in all zones. If the reserved block of numbers is 8*, the service prefix for a 384K call with 5 users could be 40880 in the 408 zone, and could be 41580 in the 415 zone. The dial string for a 384K conference call in zone 408 would be <40880><conference ID>, this eliminates the need for hopoff entries (Hopoffs are covered in Chapter 7 Call Routing), and associates the service with the zone the service resides in.

Gateway services in a multi zone network will remain consistent with the single zone model. Reserve a block of numbers for gateway services. In zones that contain gateways, off net calls will always use the local gateway. For zones without a gateway, a hopoff entry will be added, or LRQ forwarding will be used to route the call to a zone that does contain a Gateway. See Chapter 7, for more information regarding hopoffs and LRQ forwarding (Directory Gatekeeper). If the reserved block of numbers was 9*, the 128K gateway service could be 90 and 384K service could be 91. These service prefixes are configured on all gateways in all zones. In zones that have a zone prefix starting with 9 administrators must insure that the zone prefix and gateway service prefixes don't overlap. If the zone prefix is 916 a gateway service prefix of 91 cannot be used in that zone, or all calls in the zone will be routed to the gateway. In order to circumvent this problem, you can configure your Gateways service prefixes to include a # sign, such as 91#. Figure 6-1 illustrates service prefix design in a multi zone network

**Figure 6-1**


Multi Zone
Service Prefix
Design
New York
Zone Prefix 212
Service Prefixes
MCU = 21280-21289
Gateway = 90-91
Denver
Zone Prefix 720
Service Prefixes
MCU = 72080-72089
Gateway = 90-91
QoS Enabled
IP WAN
San Jose
Zone Prefix 408
Service Prefixes
MCU = 40880-40889
Gateway = 90-91

## Single Zone Dial plan:

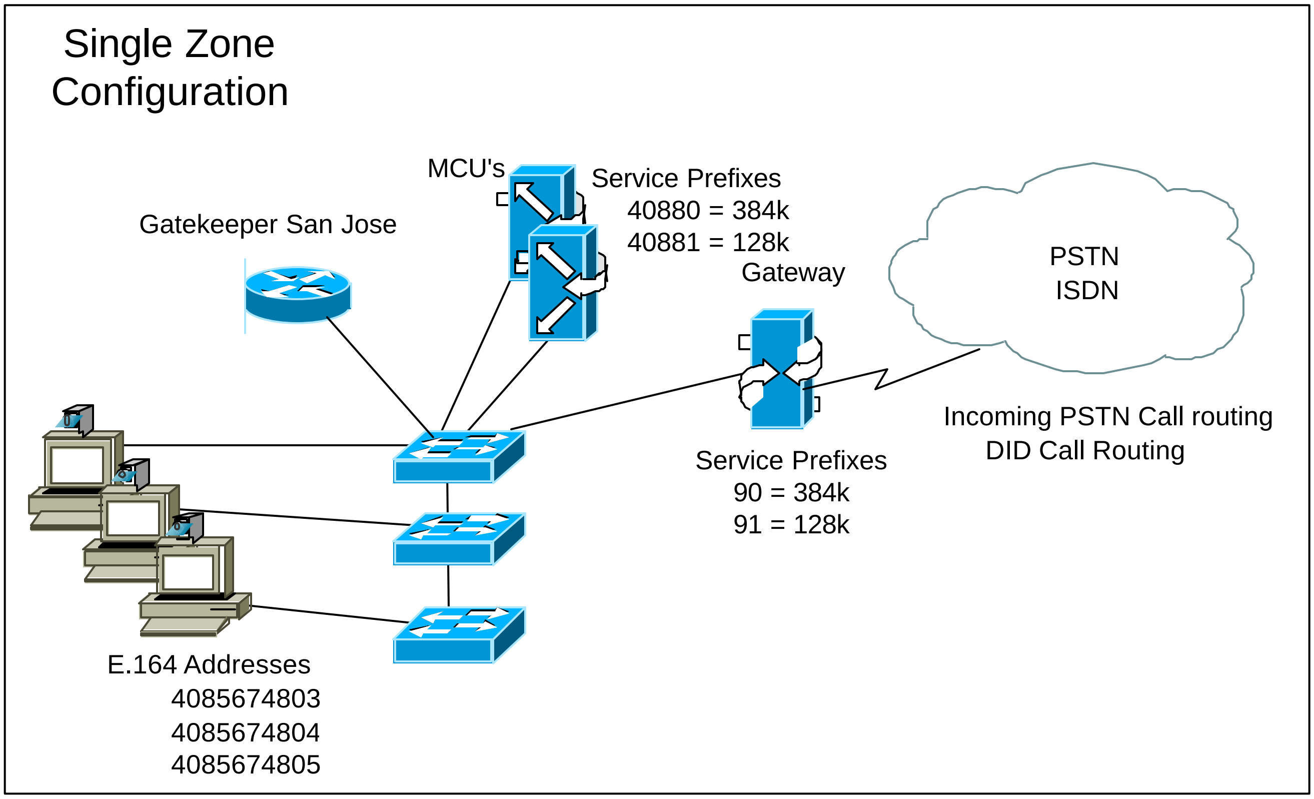
Dial plans for single zone network are fairly straightforward. There are a few rules that must be followed to ensure that call routing in a single zone will work properly. When developing a dial plan for a single zone network the following components must be considered: incoming PSTN routing method, service prefixes, and H323-ID. As a rule of thumb, the incoming PSTN routing method is a good place to start, the incoming routing method will dictate the number strings used in the dial plan. Incoming PSTN routing methods are defined in detail in Chapter 7 Call Routing. Figure 6-2 illustrates a single zone design for a campus network.

- Incoming PSTN call routing will determine the E.164 numbering structure that will be used in the dial plan. If Direct Inward Dial (DID) is used each H.323 endpoint will be assigned a valid E.164 Directory Number (DN). If IVR or TCS4 is used the administrator will decide on the E.164 number structure. It is always a good idea to use 10 digit numbers for E.164 addresses; this allows an easy migration to a multi zone dial plan. DID, IVR and TCS4 are covered in detail in Chapter 7 call routing.

- Service prefixes must not overlap with E.164 addresses, so it is a good idea to reserve a block of numbers for service prefixes. In Figure 6-2 the reserved block of numbers is 8* for MCUs and the area code is 408, the two service prefixes for the MCU are 40880 and 40881. Gateway services are 9* and do not include the area code.

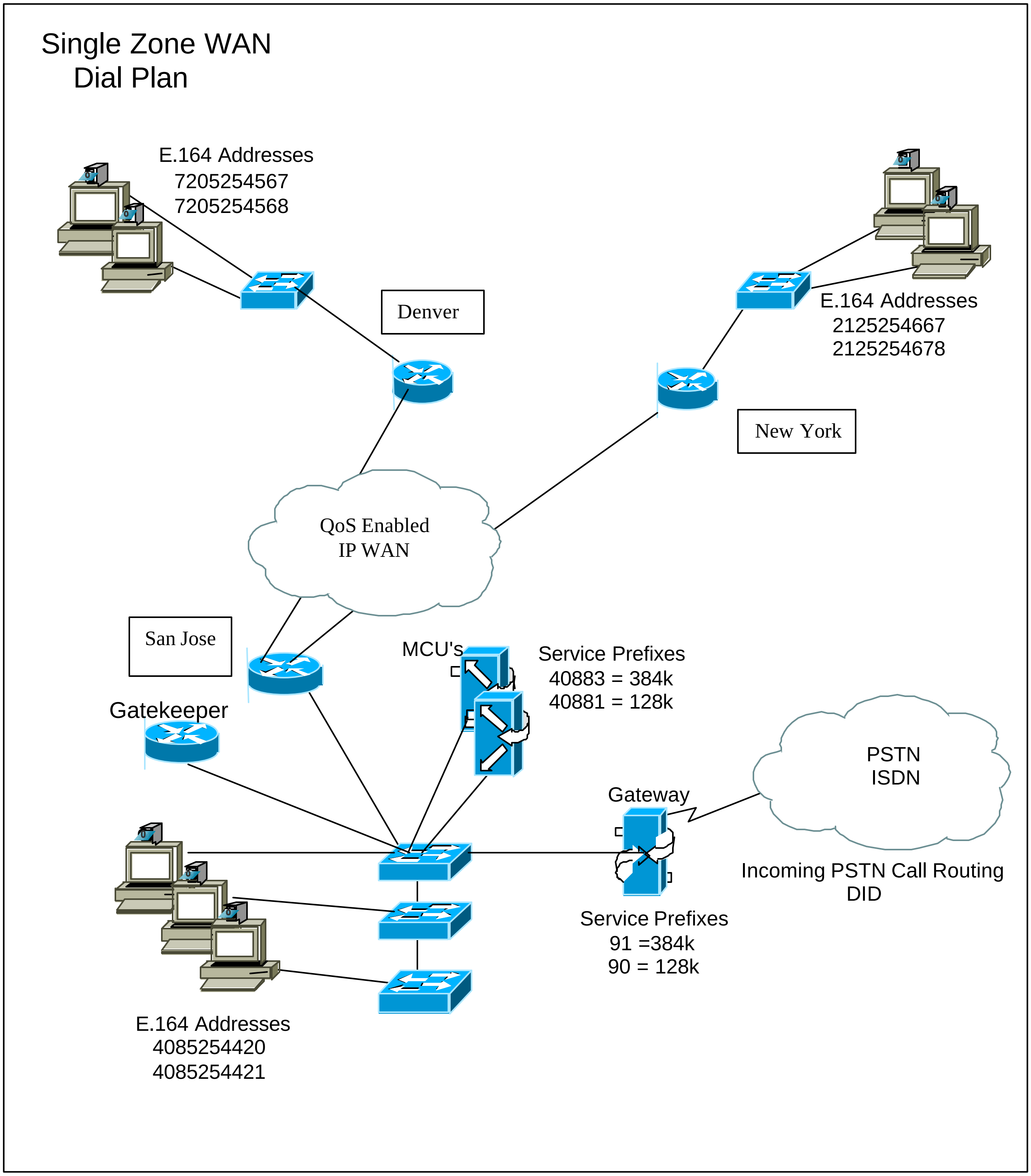
- H323-ID's are alphanumeric strings used to identify an H.323 terminal. H323-IDs are often email addresses of individual users, or conference room names for room systems. Using H323-IDs to place calls is fairly intuitive, as long as the user-to-endpoint mapping is fairly static. Some H.323 room systems are used in multiple conference rooms and naming these units can be a challenge.

**Figure 6-2**



When creating a dial plan for a single zone in a WAN environment, it is always a good idea to use a numbering scheme that allows an easy migration to a multi zone dial plan. Figure 6-3 illustrates a single zone WAN dial plan. All video terminals, gateways and MCUs will register in one zone and be routed based on the 10-digit E.164 address, H323-ID, or service prefix registered by each device.

## Figure 6-3



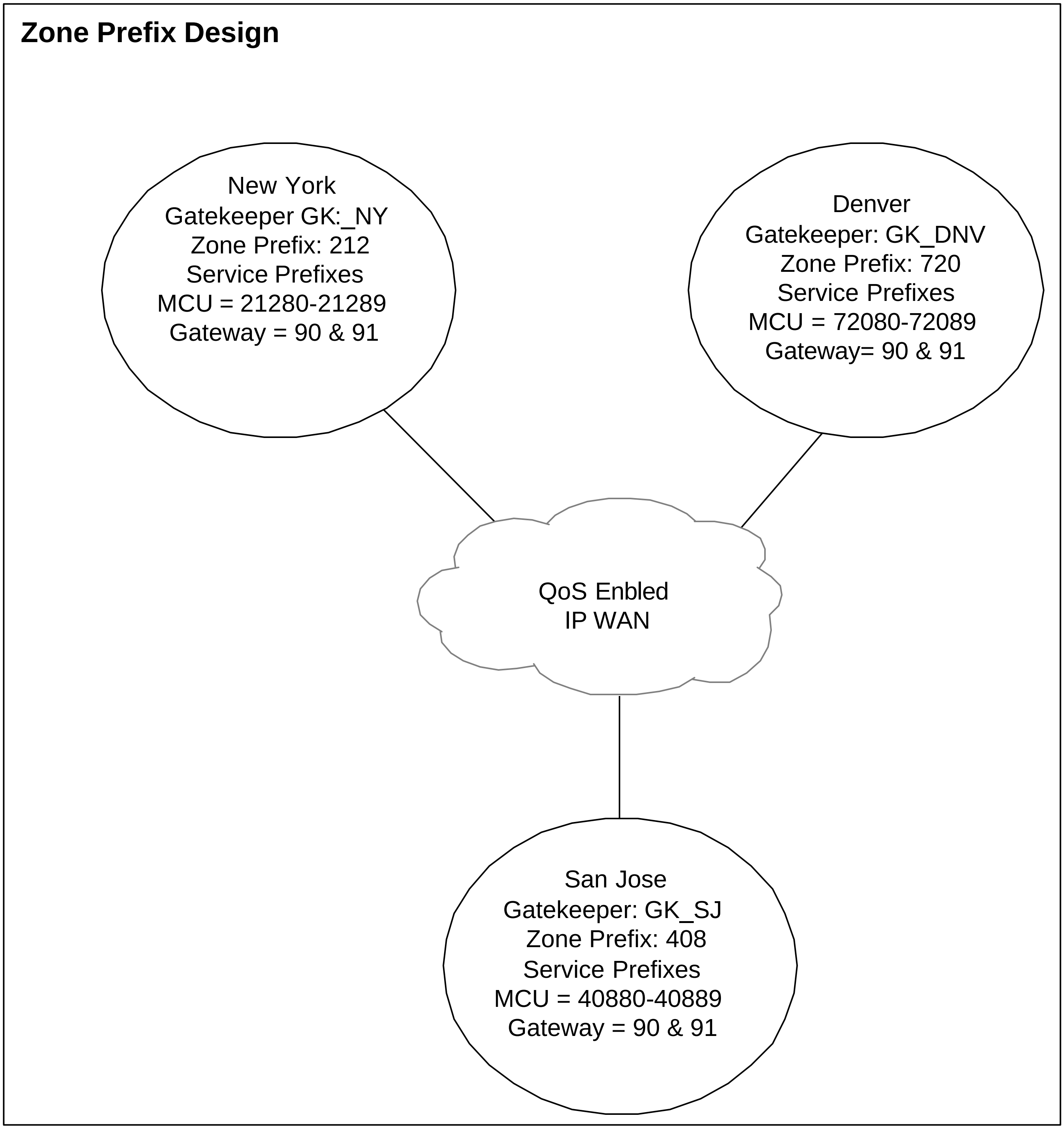
## Zone Prefix Design:

| Service Prefix | **Zone Prefix** | E.164 Address |
|---|---|---|

Zone prefixes are used in an H.323 video network to allow inter zone call routing between H.323 endpoints; the same way an area code is used in the PSTN.  Each zone on the network must have a unique zone prefix that will be used to identify the zone.  Using the local area code for the zone prefix is a recommended.  In Figure 6-4 there are three zones: Cisco San Jose campus zone 408*, Cisco New York 212*, and Cisco Denver 720*.  Zone prefixes can also be configured in the gatekeeper with dots instead of a wild card (*).  If dots are used for zone prefix entries (408…….) a second zone prefix will need to be added if an IP/VC MCU is registering in the same zone.  IP/VC MCUs register with an E.164 address that is 12-digits long starting with 7767.  Since the zone prefix now uses dots the E.164 address of any video device registering with the zone must match the number of digits defined in the zone prefix.  Adding a second zone prefix of (7767……..) will allow the MCU to register and function properly.

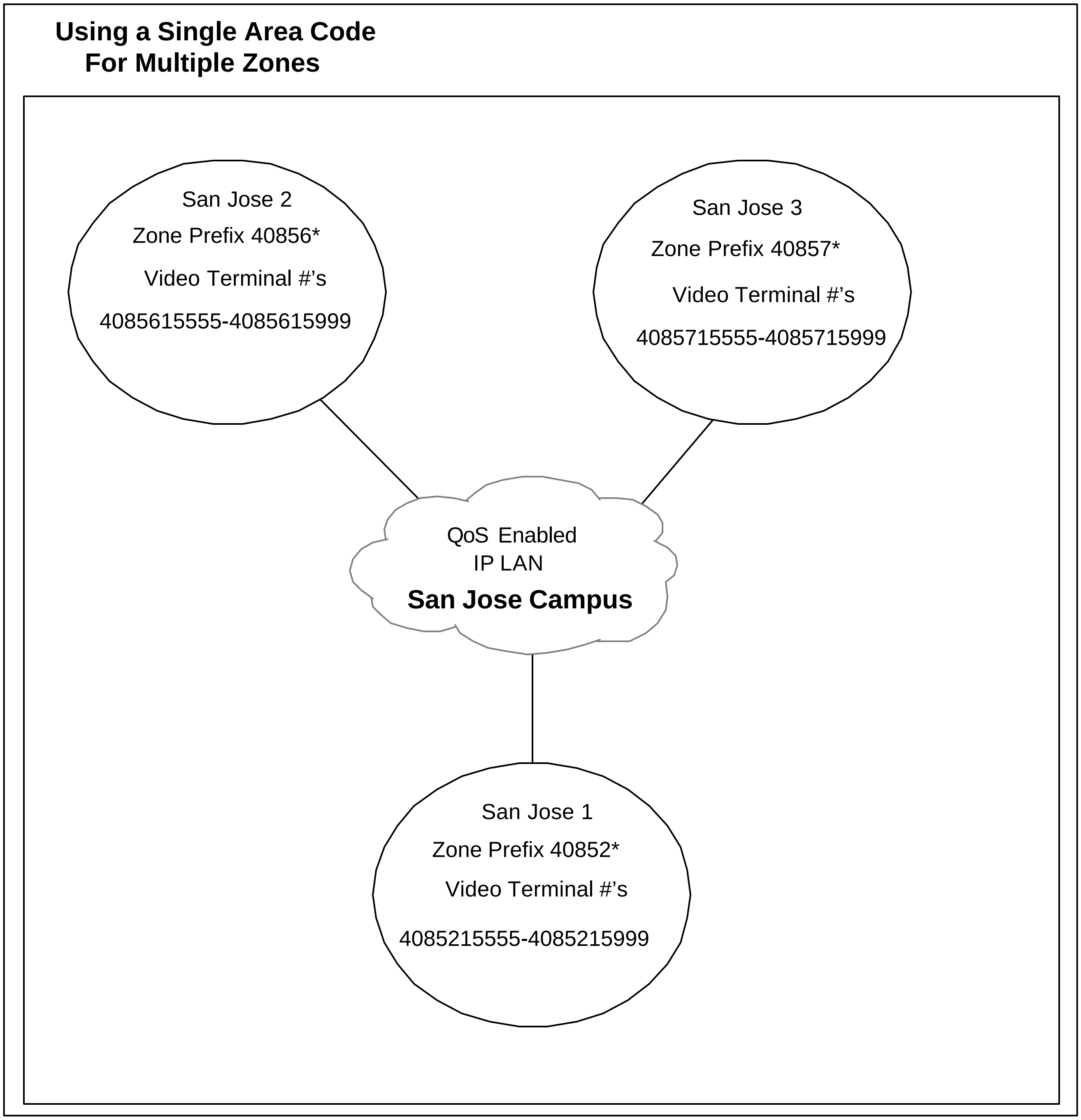
Note:  A single zone will support multiple zone prefixes.  If multiple zone prefixes are configured for a single zone an IP/VC MCU will not register with either configured zone.  For example: if a zone San Jose is configured with a zone prefix of 408* and a second zone prefix is added, (with any prefix entry) an IP/VC MCU will not register with the San Jose zone.  Currently the MCU registers with a bogus E.164 address that is 12-digits long and starts with 7767.  In order to get the MCU to register with the San Jose zone a third zone prefix must be added as (7767……..). When adding this zone prefix verify that there will not be any overlap due to the (7767……..) zone prefix.  This shouldn't cause overlap for US dial plans due to the 12-digit string, but may cause issues with international dial plans.  If overlap occurs verify the E.164 address the MCU is registering with and make the zone prefix more specific, say nine numbers and three dots.

**Figure 6-4**


Zone Prefix Design
New York
Gatekeeper GK:_NY
Zone Prefix: 212
Service Prefixes
MCU = 21280-21289
Gateway = 90 & 91
Denver
Gatekeeper: GK_DNV
Zone Prefix: 720
Service Prefixes
MCU = 72080-72089
Gateway= 90 & 91
QoS Enbled
IP WAN
San Jose
Gatekeeper: GK_SJ
Zone Prefix: 408
Service Prefixes
MCU = 40880-40889
Gateway = 90 & 91

Large sites with a need for more than one zone can still use the local area code and expand the zone prefix to include some of the E.164 address. Let's use the Cisco main campus in San Jose as an example. We need to create three zones in San Jose. One will be 40852*, the second 40856* and the third 40857*. The video terminals in each of these zones must register with the fully qualified address and start with the zone prefix. For example; a client in zone 40856* would register with 405565212. This allows the dial strings to remain consistent and expand the use of a single area code to multiple zone prefixes. Figure 6-5 illustrates this example.

**Figure 6-5**



## Multi Zone Dial Plan:

Dial plans for multi zone networks have the added complexity of zone prefixes and inter zone call routing. When developing a dial plan for a multi zone network, the following components must be considered: incoming PSTN routing method, service prefixes, zone prefixes and H323-ID's. Again, it is a good idea to start with the incoming PSTN routing method when developing the dial plan. Figure 6-6 illustrates a multi zone design using IVR and Figure 6-7 illustrates a multizone design using IVR.

- Incoming PSTN call routing will determine what E.164 numbering structure will be used in the dial plan. DID is not recommended for use as the primary incoming PSTN routing method in a multi zone network; unless there is at least one Gateway in each PSTN area code. This is because the DID number will be within one area code, but the remote zone prefix may be in a different area code. Rather than configuring your remote zone prefixes to match the area code, which would confuse the dial plan, it is recommended that you place a Gateway in each area code. It is important insure that enough DID numbers are ordered for all zones located in the area code being serviced by the gateway. The Cisco gatekeeper doesn't support digit manipulation, therefore routing incoming DID calls between zones is very difficult. There will be cases in a multi zone network where a mix of incoming call routing is used. If IVR or TCS4 is used the administrator will decide on the E.164 number structure, it is recommended that 10 digit numbers that include the zone prefix are used. Incoming call routing is covered in more detail in Chapter 7 Call routing.

- Service prefixes must not overlap with E.164 addresses, so it is a good idea to reserve a block of numbers for service prefixes. When a range of numbers is reserved for MCUs, say 8*, append the zone prefix to the reserved number to create a unique service prefix. If the zone were 408 and the reserved block of numbers was 8* the first service prefix might be 40880. An H.323 endpoint may not register with an E.164 address that starts with 40880-40889. If an MCU registers with a service prefix of 40880 in the zone, and an H.323 endpoint registers with 4088012, all calls to 4088012 will be routed to the MCU.

- Zone prefixes will also be very important in the development of the dial plan. Zone prefixes are much like area codes in the telephony world. It is recommended that local area codes be used for zone prefixes. Since area codes are unique, already defined, and people are familiar with them, it makes sense to use the local area code as the zone prefix. Again, it is up to the administrator to decide on the zone prefixes, but it is also important that the prefixes are intuitive and will continue to grow with the network. Zone prefixes must not overlap with service prefixes (if you use zone prefix plus service prefix for MCUs overlap with MCUs will not be an issue), or call routing issues will arise (see Service Prefix Design earlier in this chapter for details).

- H323-ID's are alphanumeric strings used to identify an H.323 terminal. H323-IDs are often email addresses of individual users, or conference room names for room systems. Using H323-IDs to place calls is fairly intuitive, as long as the user-to-endpoint mapping is fairly static. Some H.323 room systems are used in multiple conference rooms and naming these units can be a challenge

If IVR is the chosen method for incoming PSTN call routing, the following must be considered:

- All systems dialing in from the PSTN must support DTMF
- A private numbering plan must be implemented

If DID is the chosen method for incoming PSTN call routing, the following must be considered:

- Gateways must reside in each area code for zone prefix consistency
- Routing of MCU calls will still need to use the IVR

**Figure 6-6**
**Using IVR**

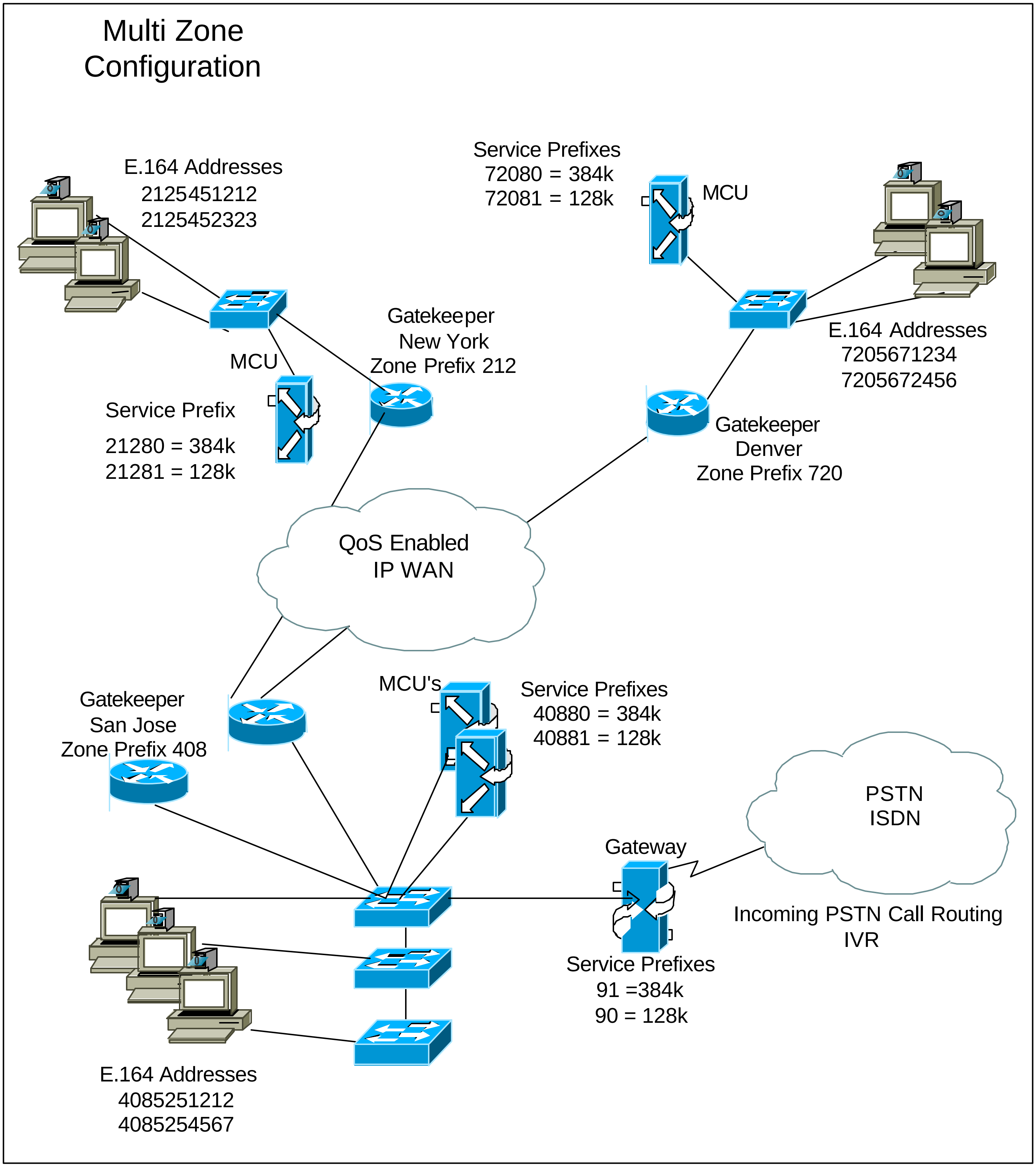
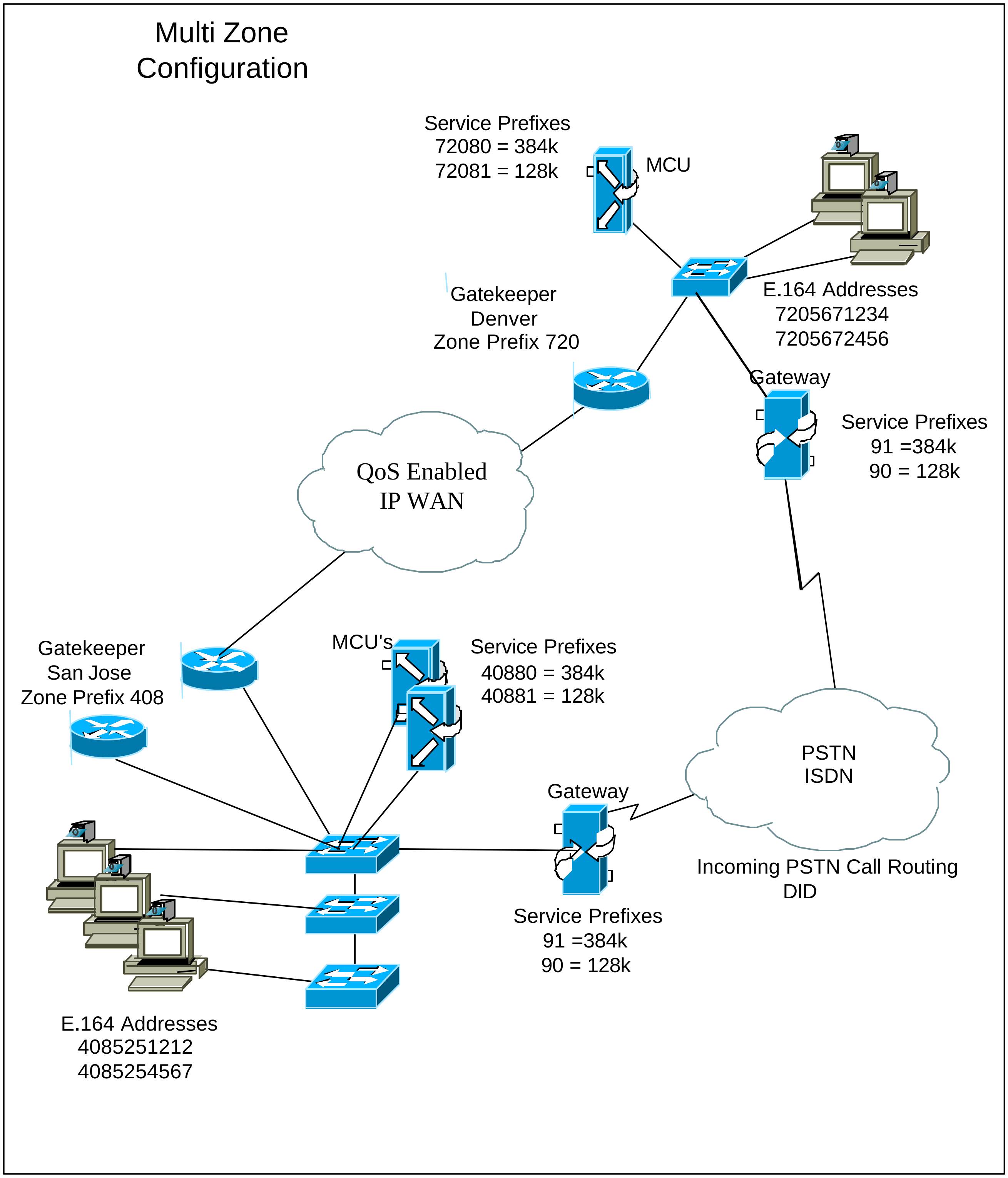


**Figure 6-7**
**Using DID**



# Chapter 7:

# Call Routing

This section covers call routing in an H.323 video networks using the Cisco gatekeeper and IP/VC equipment. Calls are routed to and from, many different devices, in a number of different ways. This section covers the different type of calls routed and methods used.

This chapter contains the following sections:

- Call Routing Scenarios
- Incoming PSTN to H.323 call routing
- Inbound PSTN call routing in a single zone
- Inbound PSTN call routing in multi zone environment
- Inter Zone Call Routing Using Hopoff Statements
- Inter Zone Call Routing Using Directory Gatekeeper

## Call Routing Scenarios:

There are four types of calls that will be routed in an H.323 network (1.) H.323 endpoint to H.323 endpoint using E.164 address, (2.) H.323 endpoint to H.323 endpoint using H323-ID, (3.) H.323 endpoint to an H.323 service (gateway or MCU), (4.) incoming PSTN to H.323 endpoint or service. Each of the four routing scenarios is discussed below.

- Routing calls between H.323 endpoints is the simplest type of call routing in an H.323 network. Dialing in a single zone requires the endpoint initiating the call to enter the E.164 address of the endpoint being called (which in most cases will be a 10-digit fully qualified E.164 address, including the zone prefix and 7-digit number of the endpoint). If the call is an inter zone call, the initiator must enter the zone prefix (if the dial plan is using 10 digit E.164 addresses the zone prefix is part of the E.164 address) and the E.164 address or the endpoint being called. Using this dial string is similar to dialing outside ones' area code in the telephony world (in multi zone networks service prefixes for MCUs and E.164 addresses should contain the zone prefix).

- Routing calls between H.323 endpoints using H323-ID requires that the calling station dial the H323-id of the video terminal being called. H323-IDs are only supported for calls from video terminal to video terminal, or video terminal to Video Terminal Adapter (VTA). When using a VTA care must be take in addressing, as some H.320 units cannot send alphanumeric strings. In these cases, E.164 addresses are the only route table mechanism. Between zones, DNS (Domain Name Service) may be used to reach the H.323-ID of an endpoint registered to a remote Gatekeeper. This is done by dialing "H323-ID@Domain" This allows the gatekeepers to resolve the remote zone destination via DNS.

- Routing calls from an H.323 endpoint to a service is also fairly simple. In a single zone an H.323 endpoint will dial the service prefix, followed by either the conference ID (for an MCU call), or ISDN telephone number of the H.320 endpoint. Routing inter zone calls to services is also done using the service prefix, but the service prefix will now contain the zone prefix for MCUs, and use hopoffs for gateways.

- Routing calls from the PSTN to H.323 endpoints or services can use one of four methods; MSN/DID, IVR, TCS4 or by using a default extension. Below each of the four PSTN to H.323 routing methods will be defined, and then applied to a single zone and multi zone environment.

Figure 7-1 illustrates a multi zone network with Video terminals and services in each zone. Table 7-1 shows the dial strings for the four Intra and Inter zone call types. Below dial strings for the scenarios in Figure 7-1 are listed.

1. H.323 endpoint to H.323 endpoint:
   **Intra zone call tsmith to jbank**: tsmith dials 4085248071
   **Inter zone call tsmith to jcox:** tsmith dials 7207125543

2. H.323 endpoint to H.323 endpoint using H323-ID:
   **Intra zone call tsmith to jbank**: tsmith dials jbank@cisco.com
   **Inter zone call tsmith to jcox**: tsmith dials jcox@cisco.com

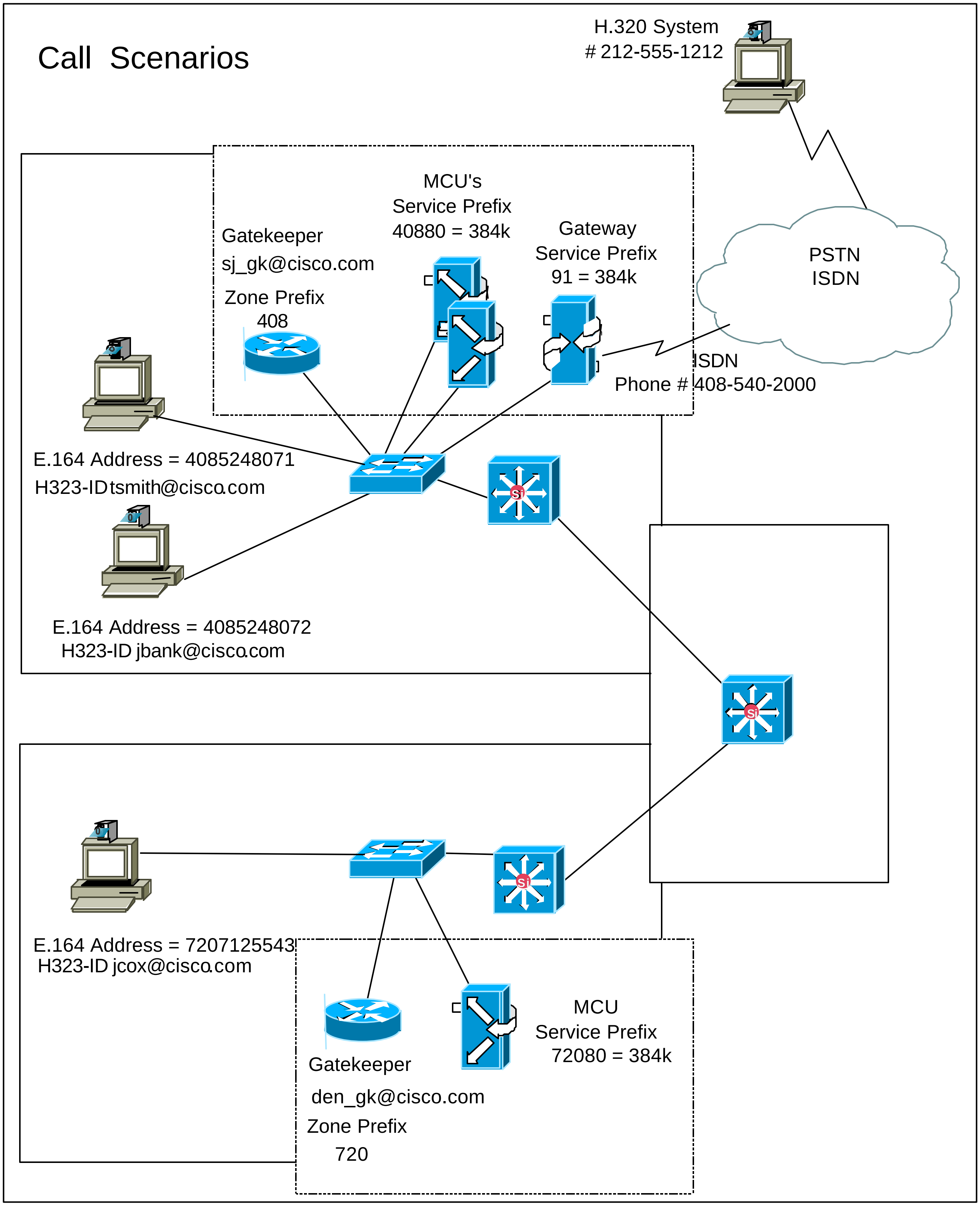
3. H.323 endpoint to service:
   **Intra zone call tsmith to H.320 system**: tsmith dials 91212555212
   **Inter zone call jcox to H.320 system**: jcox dials 91212555212
   *Gateway calls will always use the local gateway if one is present.

4. PSTN endpoint to H.323 endpoint or service (using IVR see PSTN to H.323 call routing):
   **Intra zone call H.320 system to tsmith**: H.320 system dials 4085402000, IVR answers, and the H.320 system enters 4085248071. Or, if DID is enabled to tsmith: H.320 system dials 4085248071 directly
   **Intra zone call H.320 system to 408 MCU conference 40880123**: H.320 system dials 4085402000, IVR answers, and the H.320 system enters 40880123. (IVR should be used for routing calls to an MCU conference, for DID and IVR deployments)
   **Intra zone call H.320 system to jcox:** H.320 system dials 4085402000 followed by 7207125543. (if a Gateway existed in the 720 area code, DID could be enabled to jcox instead of having to dial the 408 Gateway, and use IVR to reach jcox in the 720 zone).
   **Inter zone call H.320 system to MCU conference72080111**: H.320 system dials 408540200 followed by 72080111. (IVR should be used for routing calls to an MCU conference, for DID and IVR deployments)

**Table 7-1**

| | | |
|---|---|---|
| **Intra Zone Calls** | | |
| **Call from** | **Call to** | **Dial String** |
| **H.323 Endpoint** | **H.323 Endpoint** | **<E.164 address> or <H323-ID>** |
| **H.323 Endpoint** | **Service** | **<Service Prefix> <Conference ID or PSTN E.164 address>** |
| **Service** | **H.323 Endpoint** | **<E.164 address>** |
| **Service** | **Service** | **<Service Prefix> <Conference ID or PSTN E.164 address>** |
| **Inter Zone Calls** | | |
| **Call from** | **Call to** | **Dial Sting** |
| **H.323 Endpoint** | **H.323 Endpoint** | **< Zone prefix +E.164 address> or <H323-ID>** |
| **H.323 Endpoint** | **Service** | **<Zone Prefix/Service Prefix> <Conference ID or PSTN E.164 address>** |
| **Service** | **H.323 Endpoint** | **<Zone Prefix/E.164 address>** |
| **Service** | **Service** | **<Zone Prefix/Service Prefix> <Conference ID or PSTN E.164 address>** |

## Figure 7-1


Call Scenarios
H.320 System
# 212-555-1212
MCU's
Service Prefix
40880 = 384k
Gatekeeper
sj_gk@cisco.com
Zone Prefix
408
Gateway
Service Prefix
91 = 384k
PSTN
ISDN
ISDN
Phone # 408-540-2000
E.164 Address = 4085248071
H323-IDtsmith@cisco.com
E.164 Address = 4085248072
H323-ID jbank@cisco.com
E.164 Address = 7207125543
H323-ID jcox@cisco.com
Gatekeeper
den_gk@cisco.com
Zone Prefix
720
MCU
Service Prefix
72080 = 384k

## Incoming PSTN to H.323 call routing:

There are multiple methods for routing calls from the PSTN to H.323 endpoints and services. An H.323 video network may contain one or more of the available routing methods (MSN/DID, IVR, TCS4, and default extension). Each routing method has advantages over the others in different situations. Each routing method is defined below.

### MSN (Multiple Subscriber Numbering) \ DID (Direct Inward Dial)

Multiple Subscriber Numbering (MSN) is a group of phone numbers assigned to a single ISDN BRI line. MSN is not available in most regions of the U.S., Canada, or South America, but is widespread in Europe.

Direct Inward Dial (DID) is support on primary rate interface (PRI) lines. DID allows multiple Directory numbers to be assigned to a single PRI line. DID is supported throughout the US and Europe.

### IVR (Interactive Voice Response)

IVR is a widely deployed automated call answering system that responds with a voice menu, allowing the H.320 endpoint to access H.323 endpoints by entering an extension from a keypad. When an incoming call arrives, the IVR answers the call, asks for the extension, the caller enters the E.164 address, and the call is transferred to the appropriate H.323 endpoint. Using IVR requires the calling H.320 endpoint to support DTMF. Most legacy room systems support DTMF (see chart below for DTMF support).

### TCS4

TCS4 is a special method for routing incoming H.320 video calls using extensions. TCS4 allows direct extension dialing to an H.323 endpoint on the LAN. H.323 endpoints on the LAN register to the gatekeeper with an E.164 number. When an H.320 endpoint dials a gateway's phone number followed by a TCS4 delimiter and the E.164 number, the call is routed directly to the corresponding H.323 endpoint. TCS4 is fairly new, and only some of the H.320 endpoints permit the user to enter a TCS4 extension when dialing (see chart below for TCS4 support). Due to the limited support for the TCS4 standard in H.320 devices TCS4 is not frequently used for incoming call routing, and therefore, DID or IVR are typically a better choices.

### Default Extension

Entering a Default Extension in the gateway will force all calls received by the video gateway to be routed directly to a default E.164 address. Default Extension can also be used in conjunction with any of the routing methods mentioned above. If the call can't be routed by one of the above methods the call will then be forwarded to a default address.

Each routing method defined above has advantages over the others in different environments. A single H.323 network may implement one or more of the routing methods defined above. Below each method will be discussed in the context of a single zone and a multi zone network.

## Inbound PSTN Call Routing in a Single Zone Network:

Routing calls from the PSTN to H.323 endpoints and services in a single zone network can be done with any of the methods defined above. Each method offers different functions and numbering structures that are described below.

- Using DID in a single zone network allows administrators to order blocks of DID numbers, and assign each H.323 endpoint a DID number to be used for its E.164 address. This allows H.320 users and H.323 users to dial the same number to access an H.323 endpoint (this assumes that in most cases 10-digits are being passed from the carrier, and the video terminals are registered with the 10-digit numbers). DID can also be used for MCU conferences, but In order to route calls to an MCU service in a zone, zone prefix, service prefix and, the conference ID must together match one of the DID numbers associated with the ISDN line. This disables the use of add-hoc conference id's created by the users on the MCU, but may be preferable since DID may be desired over using IVR to reach these conferences. This does however require that conference ID match the statically registered directory number. DID call routing is very desirable, since the dial strings are exactly the same as those used in the telephony world, but routing H.323 service prefixes can become complex when using DID call routing.

- Internal Voice Response (IVR) allows administrators to define the dial plan. E.164 addresses can be four digit extensions or 10 digit directory number numbers (10 digit directory numbers are recommended). When routing incoming PSTN calls using IVR, the call initiator must dial the directory number of the PRI gateway, and enter the E.164 address, or service prefix dial string after the IVR has answered. IVR requires DTMF support on the dialing endpoint, and some older legacy H.320 systems do not support DTMF (see Table 7-2 TCS4/DTMF support).

- When using TCS4 to route incoming calls the numbering plan, is again decided by the administrator. When using TCS4 the initiator dials the directory number of the gateway, a TCS4 delimiter (the delimiter is configured in each video gateway, the options are # or *), and the E.164 address or service. Using TCS4 requires the dialing endpoint to support TCS4 (see Table 7-2 TCS4/DTMF support). TCS4 is not a commonly used routing method.

- Default extension is usually used in special cases such as call center applications, or to direct calls to a single H.323 video terminal.

Note: All of the dial in methods defined above are mutually exclusive, and multiple incoming routing methods can be implemented on the same gateway. If an incoming PSTN call arrives at a gateway supporting all of the routing methods defined above the gateway will try to first resolve the address using MSN/DID, then IVR, followed by TCS4, and lastly using a default extension. A good example of a gateway supporting multiple incoming call routing methods is in a DID environment. It is not recommended that ad hoc MCU calls be assigned a DID number, so incoming calls to an MCU will use IVR, and incoming calls to video terminals will be routed using DID.

## Table 7-2

This table is a result of industry research performed by Cisco, in an effort to summarize each of our partners' capabilities as they relate to interoperability with the IP/VC Gateways. The information included in the table below is subject to change, and you should contact the vendor directly for updated information

| **Picture Tel** | **DTMF** | **SW Ver.** | **TCS4** | **SW Ver.** |
|---|---|---|---|---|
| Concorde 4500 | Yes | 6.1 | Yes | 6.3 |
| Venue 2000 | Yes | 1.3 | No | |
| Proshare 500 | Yes | 5 | No | |
| Teamstation | Yes | 4 | No | |
| SwiftSet II | Yes | 1.04 | No | |
| **VTEL** | | | | |
| Galaxy 725 | Yes | 1 | Yes | 1 |
| Galaxy 755 | Yes | 1 | Yes | 1 |
| Galaxy 2500 | Yes | 1 | Yes | 1 |
| Galaxy 5500 | Yes | 1 | Yes | 1 |
| Gateway | Yes | 1.2 | Yes | 1.1 |
| Smart Station | Yes | 5 | No | |
| WG500 | Yes | 5 | No | |
| ESA TC1000 | No | | No | |
| ESA TC2000 | No | | No | |
| ESA TC5000 | No | | No | |
| Smart Link MCS | No | | No | |
| Settop 250 | No | | No | |
| **VCON** | | | | |
| Escort 25 | Yes | 4.01 | Yes | 4.01 |
| Cruiser 75 | Yes | 4.01 | Yes | 4.01 |
| Cruiser 150 | Yes | 4.01 | Yes | 4.01 |
| Cruiser 384 | No | | Yes | 4.01 |
| Media Connect 8000 | No | | Yes | 4.01 |
| Media Connect 6000 | No | | Yes | 2 |
| **Tandberg** | | | | |
| Vision 600 | Yes | Any | No | |
| Vision 770 | Yes | Any | No | |
| Vision 1000 | Yes | Any | No | |
| Vision 2000 | Yes | Any | No | |
| Vision 2500 | Yes | Any | No | |
| Vision 5000 | Yes | Any | No | |
| **Zydacron** | | | | |
| Z350 Windows 98 | Yes | 2.2 | Yes | 2.2 |
| Z350 for NT | Yes | 2.3 | Yes | 2.3 |
| OnWAN240/250 Win 95 | Yes | 2.04 | Yes | 2.04 |

| | | | | |
|---|---|---|---|---|
| OnWAN250 for OS/2 | Yes | 2 | Yes | 2 |
| OnWAN240/250 Win NT | Yes | 2.02 | Yes | 2.02 |
| Z220 Plus for Win 95 | Yes | 2 | Yes | 2 |
| Z360 for Win NT | Yes | 1.1 | Yes | 1.1 |
| **Polycom** | | | | |
| ViewStation SP | Yes | 5.X | Yes | 5.X |
| ViewStation FX | Yes | 6.X | Yes | 6.X |
| ViaVideo | Yes | 1.5X | Yes | 1.5X |

## Incoming PSTN Call Routing in a Multi Zone Network:

Call routing in a multi zone network becomes more complicated due to the advent of zone prefixes, and inter zone routing of service prefixes. For example: the executive staff of a company may reside in a single zone, to keep the dial strings simple DID may be implemented in the executive zone. Other zones on the network may use IVR due to the lack of video gateway services in every zone. Using the dial plans outlined in this document dial strings stay consistent across all zones.

- If Direct Inward Dialing (DID) is going to be used to route calls from the PSTN to the H.323 endpoints and services, each E.164 address and service will be a valid DID number associated with an PRI line attached to an IP/VC gateway. In order to use DID in a multi zone network where zones may reside in different geographic regions, PSTN area codes, and "lata" boundaries, requires a video gateway in each area code.

- IVR allows administrators to define the number structure of the dial plan. E.164 addresses can be four digit extensions or 10 digit directory numbers (10 digit directory numbers are recommended). IVR is the easiest method for routing incoming PSTN calls in a multi zone network. When using IVR calls are terminated at the gateway, and then the E.164 address or service is entered. If the call is in local zone only the E.164 address or service is entered. If the call is going to another zone the caller will enter the zone prefix followed by the E.164 address. Services hosted on a remote MCU will be dialed the same way, that is zone prefix + service prefix + conference id. IVR requires DTMF support from the dialing endpoint, and some older legacy H.320 systems do not support DTMF (see Table 7-2 TCS4/DTMF support).

- When using TCS4 the dial string from the H.320 endpoint will contain the ISDN directory number for the gateway, followed by a TCS4 delimiter, and the E.164 address of the H.323 endpoint. If the incoming call is destine for an H.323 endpoint outside of the local zone the zone prefix will needed to be added to the dial string. Using TCS4 requires the dialing endpoint to support TCS4 (see Table 7-2TCS4/DTMF support). TCS4 is not a commonly used routing method, IVR is recommended over TCS4.

- Default extension is usually used in special cases such as call center application, and routing calls to a single H.323 endpoint.

## Inter Zone Call Routing Using Hopoff Statements:

Hopoff statements are added in the gatekeeper and allow calls to be routed Inter zone without using a zone prefix. Hopoffs are used for routing of gateway services since the service has no association with the zone the gateway resides in. Strategically deploying Gateways in major sites, and using hopoff statements in all smaller "stub" zones that do not contain a Gateway creates a common dial plan. Then users regardless of what zone they are in are taught to dial a common service prefix to access the outside world. The use of the hopoff statement eliminates the need for users in a stub zone to dial the zone prefix of the zone that contains the Gateway. Hopoffs over ride the gatekeeper parse order and direct calls with the defined service to a specific zone. Hopoff statements are configured in the gatekeeper using the following command. MCUs do not require hopoff statements since the zone prefix is always embedded into the service prefix.

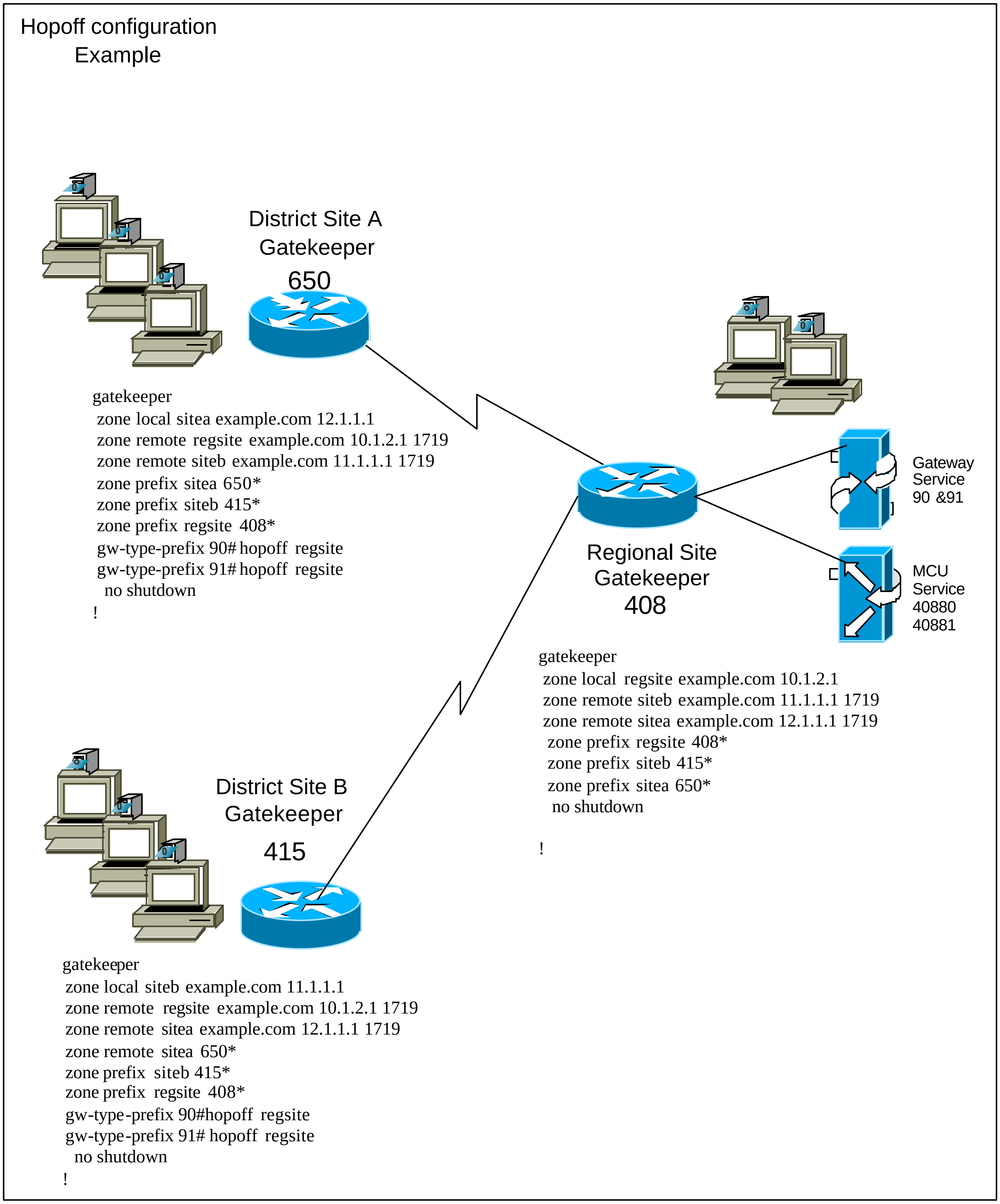
**gw-type-prefix** *<prefix #>* **hopoff** *<gatekeeper name>*

Note: When creating multiple zones on a single router and registering MCUs or gateways in any of the zones, hopoff commands must be entered for each service prefix. Routing of service prefixes between local zones requires a hopoff.

In figure 7-2 District Site A and District site B have hopoffs configured to forward all gateway calls, service prefix 90# &91# to the regional site. These hopoff statements will forward calls matching 90#* and 91#* to the regional site.

**Figure 7-2**

Hopoff configuration Example



```
gatekeeper
 zone local sitea example.com 12.1.1.1
 zone remote regsite example.com 10.1.2.1 1719
 zone remote siteb example.com 11.1.1.1 1719
 zone prefix sitea 650*
 zone prefix siteb 415*
 zone prefix regsite 408*
 gw-type-prefix 90# hopoff regsite
 gw-type-prefix 91# hopoff regsite
  no shutdown
!
```

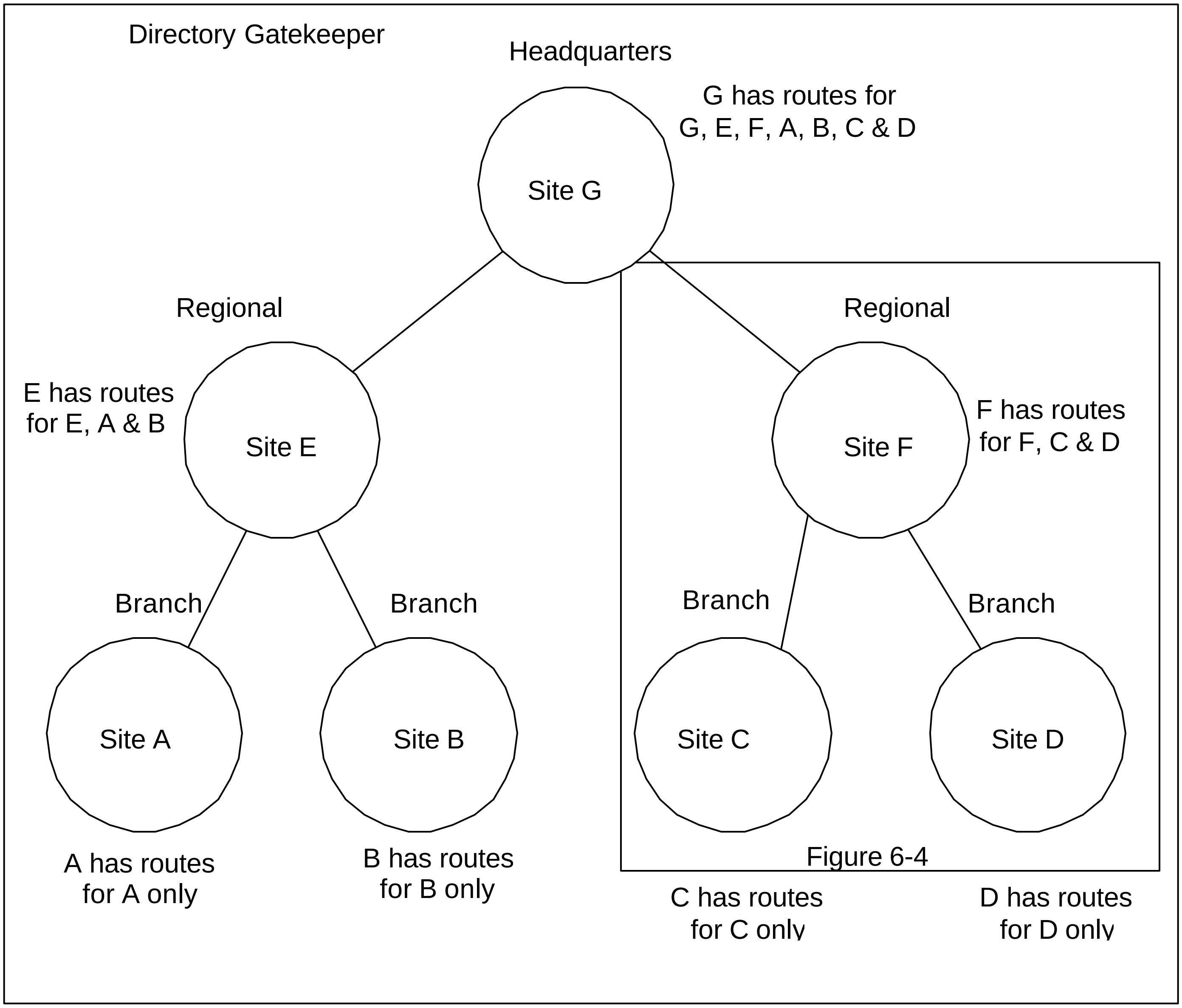
```
gatekeeper
 zone local regsite example.com 10.1.2.1
 zone remote siteb example.com 11.1.1.1 1719
 zone remote sitea example.com 12.1.1.1 1719
  zone prefix regsite 408*
  zone prefix siteb 415*
  zone prefix sitea 650*
   no shutdown

!
```

```
gatekeeper
 zone local siteb example.com 11.1.1.1
 zone remote regsite example.com 10.1.2.1 1719
 zone remote sitea example.com 12.1.1.1 1719
 zone remote sitea 650*
 zone prefix siteb 415*
 zone prefix regsite 408*
 gw-type-prefix 90#hopoff regsite
 gw-type-prefix 91# hopoff regsite
   no shutdown
!
```

## Inter Zone Call Routing Using a Directory Gatekeeper:

Currently there is no gatekeeper protocol that allows gatekeepers to update each other with routing information. This implies a full-mesh topology where every gatekeeper must be statically configured to know about every other gatekeeper that it is going to route calls to. In effect all gatekeepers must be known to each other. This poses scalability problems when a new zone or service is added, the administrator must add an entry in every gatekeeper for the new zone or service. By using a directory gatekeeper and LRQ forwarding, a hierarchical gatekeeper design can limit the administrative overhead in a large multi zone network. LRQ forwarding allows an administrator to create a directory gatekeeper that maintains all zone prefixes for the network or subset of the network. In Figure 7-3 sites A, B, C, and D are configured to forward all LRQs that can’t be resolved locally to a directory gatekeeper sites (E and F).

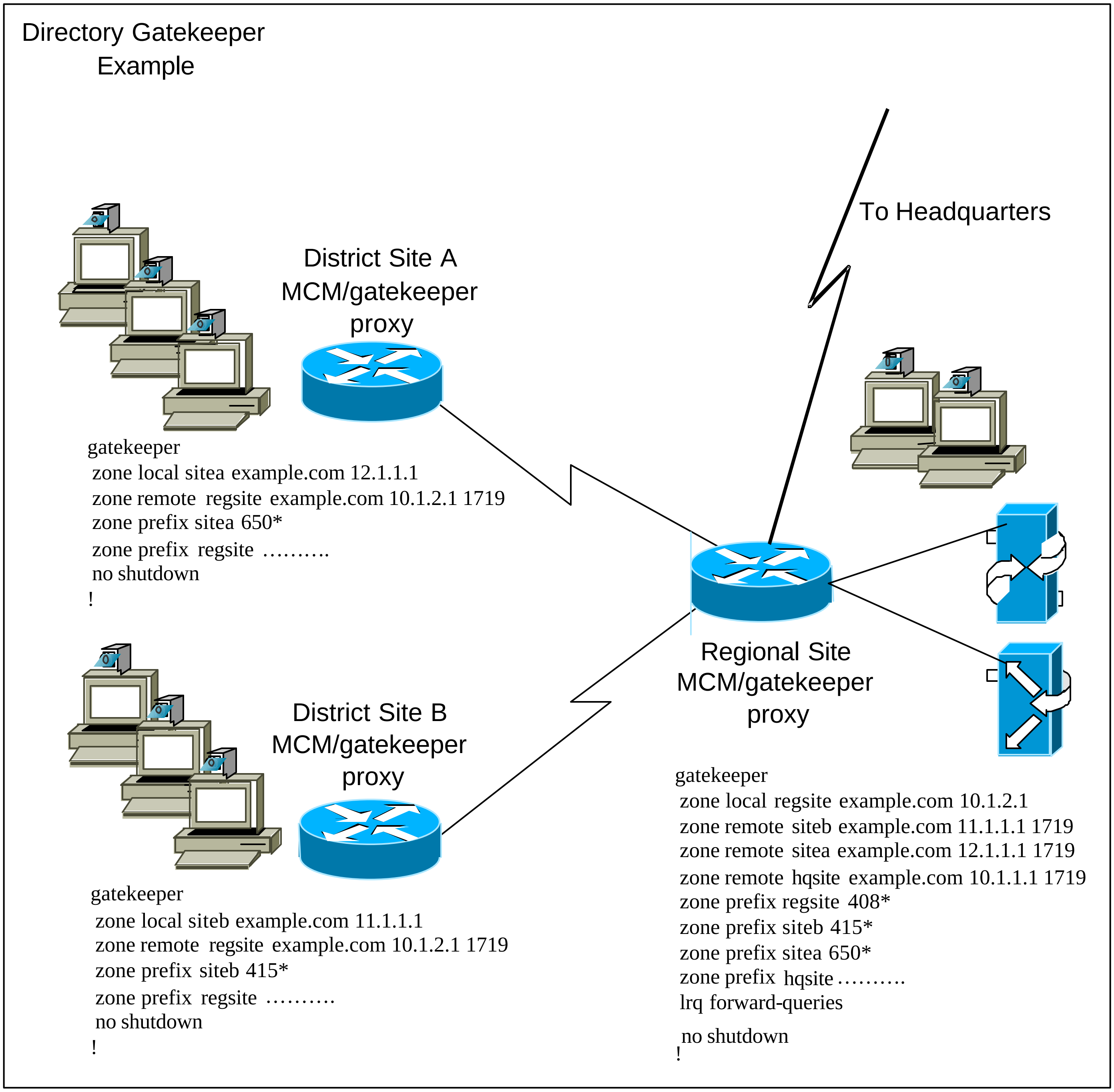
**Figure 7-3**



In figure 7-4 there are three zones, two district zones and a regional zone that has a connection back to headquarters. Each district zones contains information about its local zone only. The command line <***zone prefix regsite ……….***> routes any call placed, with no match in the local zone, to the regional site.

The regional site contains the routing information for its own zone, as well as, the two district zones below it. Zone prefix and hopoff statements will be added to the regional site as they are added to the network. There is also a< ***zone prefix hqsite ……….***> entry in the regional gatekeeper that forwards any calls with no match to the headquarters gatekeeper. If LRQs are going to be forwarded past the directory gatekeeper an< ***lrq forward-queries***> >entry must be added to the gatekeeper or LRQ's will not be forwarded past the directory gatekeeper. This model can be expanded on in a large network to make an H.323 network more manageable.

**Figure 7-4**



```
gatekeeper
 zone local sitea example.com 12.1.1.1
 zone remote  regsite  example.com 10.1.2.1 1719
 zone prefix sitea 650*
 zone prefix  regsite  ……….
 no shutdown
!
```

```
gatekeeper
 zone local siteb example.com 11.1.1.1
 zone remote  regsite  example.com 10.1.2.1 1719
 zone prefix siteb 415*
 zone prefix  regsite  ……….
 no shutdown
!
```

```
gatekeeper
 zone local  regsite  example.com 10.1.2.1
 zone remote  siteb example.com 11.1.1.1 1719
 zone remote  sitea  example.com 12.1.1.1 1719
 zone remote  hqsite  example.com 10.1.1.1 1719
 zone prefix regsite  408*
 zone prefix siteb 415*
 zone prefix sitea 650*
 zone prefix  hqsite ……….
 lrq forward-queries
 no shutdown
!
```

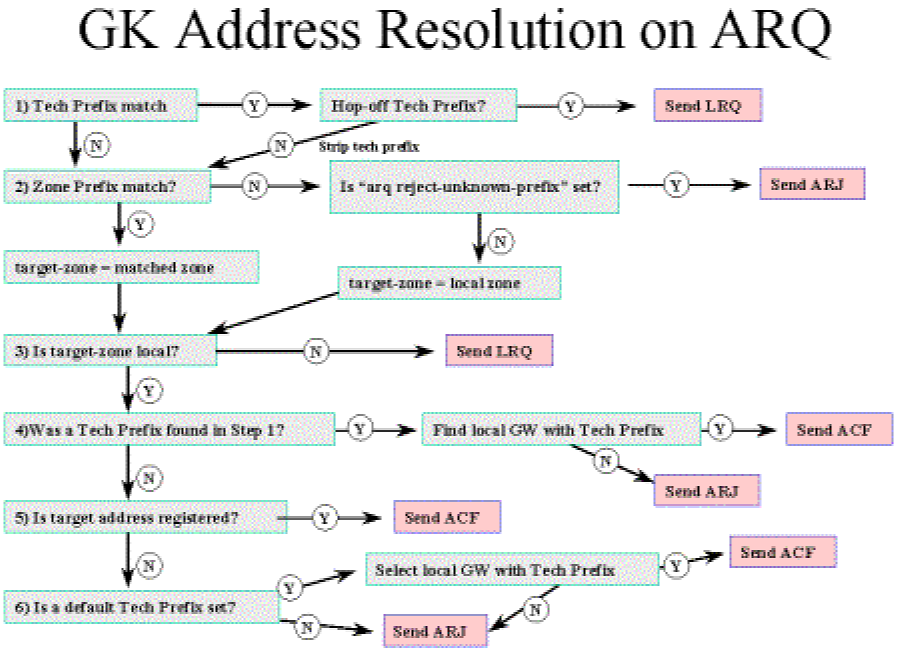
Note: When configuring directory gatekeeper the use of a wildcard (*) as the directory gatekeeper entry is not recommended. If the wildcard (*) is used major call routing issues will arise. In figure 7-4 the directory gatekeeper entry is <zone prefix regsite ………> this allows any 10-digit dial string that is not matched locally to be forwarded to the directory gatekeeper. If there is a need for users to dial 11 or 12-digit dial strings multiple zone prefix entries may be entered for the directory gatekeeper. In deployments that support international locations there will more than likely be multiple zone prefix entries for the directory gatekeeper.

If a root zone contains a video gateway and multiple directory gatekeeper zone prefixes are configured a hopoff may need to be added to the configuration. If any of the DGK zone prefix lengths match the dial string, minus the service prefix, the call will be forwarded to the directory gatekeeper. For example: if a local gateway service prefix is 9#, PSTN calls will be either 9-digits (local calls) or 12-digits (long distance) including the service prefix. When the gatekeeper starts to parse the dial string it will strip the service prefix and start looking for a match. In the example above local calls will be parsed on 5-digits and long distance calls will be parsed on 11-digits. If the gatekeeper configuration contains a directory gatekeeper entry with 5 dots or 11 dots a hopoff will be needed. The same rule applies to MCUs, but in most cases MCU calls are parsed on 5-digits or less, and most directory gatekeeper zone prefix entries are matched on 10-digits or more. Figure 7-5 illustrates the configuration of a root zone containing multiple directory gatekeeper zone prefix entries and a hopoff for 9#. The reason for the hopoff is to eliminate long distance calls (which are parsed on 11-digits) from matching the DGK zone prefix entry with 11 dots. Figure 7-6 and 7-7 illustrate the parse order for ARQ's and LRQ's in the Cisco gatekeeper.

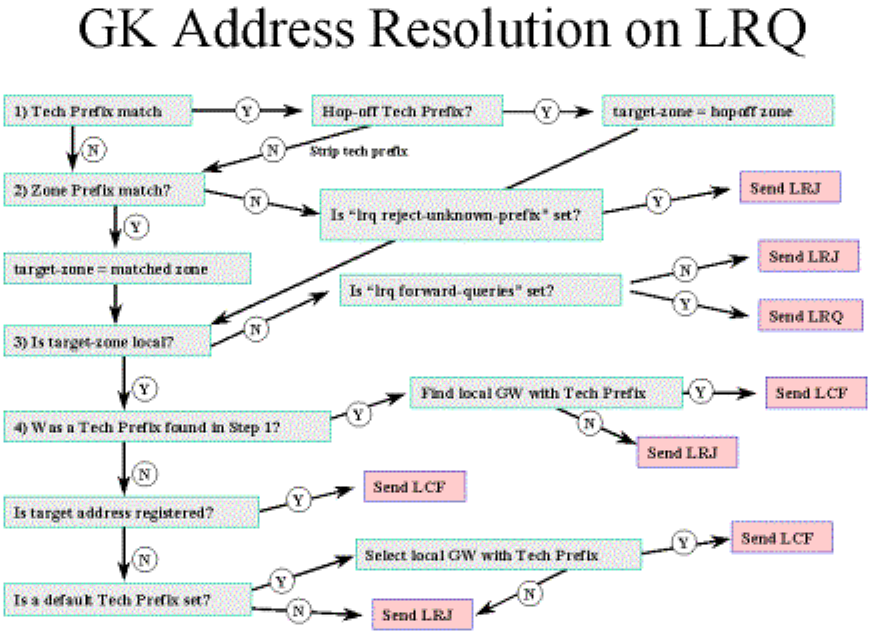
## Figure 7-5

```
gatekeeper
 zone local HKG cisco.com 10.1.3.1
 zone remote APAC_DGK cisco.com 10.1.2.1
 zone prefix HKG 852*
 zone prefix APAC_DGK ..........
 zone prefix APAC_DGK ...........    (This entry would match long distance PSTN calls to a gateway)
 zone prefix APAC_DGK ............
 gw-type-prefix 9#* hopoff HKG    (this entry overrides the parse order)
 no use-proxy HKG default inbound-to terminal
 no use-proxy HKG default outbound-from terminal
 bandwidth remote 1000
 no shutdown
```

## Figure 7-6


GK Address Resolution on ARQ
1) Tech Prefix match
Y
Hop-off Tech Prefix?
Y
Send LRQ
N
N
Strip tech prefix
2) Zone Prefix match?
N
Is "arq reject-unknown-prefix" set?
Y
Send ARJ
Y
N
target-zone = matched zone
target-zone = local zone
3) Is target-zone local?
N
Send LRQ
Y
4)Was a Tech Prefix found in Step 1?
Y
Find local GW with Tech Prefix
Y
Send ACF
N
Send ARJ
N
5) Is target address registered?
Y
Send ACF
N
Send ACF
Select local GW with Tech Prefix
Y
Y
6) Is a default Tech Prefix set?
N
Send ARJ
N

## Figure 7-7


GK Address Resolution on LRQ
1) Tech Prefix match
Y
Hop-off Tech Prefix?
Y
target-zone = hopoff zone
N
N
Strip tech prefix
2) Zone Prefix match?
N
Is "lrq reject-unknown-prefix" set?
Y
Send LRJ
Y
target-zone = matched zone
Is "lrq forward-queries" set?
N
Send LRJ
Y
Send LRQ
3) Is target-zone local?
N
Y
Find local GW with Tech Prefix
Y
Send LCF
4) Was a Tech Prefix found in Step 1?
Y
N
Send LRJ
N
Send LCF
Is target address registered?
Y
N
Select local GW with Tech Prefix
Y
Send LCF
Is a default Tech Prefix set?
Y
N
Send LRJ
N

# Chapter 8:

# Cisco Video Infrastructure Components:

This section will cover the Cisco video infrastructure components, and the design of the network in regards to these components. The Cisco video Infrastructure consists of the IP/VC 3510 MCU, IP/VC 352X gateways, IP/VC 3530 VTA and the Multimedia Conference Manager (MCM).

This Chapter contains the following sections:

- Overview
- MCUs
- Video Gateways
- Video Terminal Adapters (VTA)
- Multimedia Conference Manager

## Overview:

The video infrastructure design is a very important element in an H.323 video network. In the H.320 circuit switched network, MCUs and H.320 endpoints are connected directly to the switched network. In the past an MCU may have had multiple PRI connections into the switched network, which users would dial into for multipoint access. The switched network would supply a dedicated transport with guaranteed bandwidth and predictable delay. Now that Video is being moved onto IP networks that share bandwidth with data, placement of video infrastructure components becomes very important. Installing a central MCU and or gateway in an IP environment will not always work. Bandwidth in an IP network is not dedicated to each video device on the network, therefore it is important to design the network accordingly.

## Multipoint Conference Unit (MCU) 3510:

The Cisco IP/VC 3510 allows conferences involving three or more endpoints. The MCU has one 10/100 Mbps Ethernet connection, and supports video data rates from 128kbps to 1.5Meg as well as G.711 based voice. The 3510 supports both voice activated and continuous presence calls. Configuration of the MCU will depend on the desired function and network layout. The IP/VC 3510 was designed to support ad hoc conferences with an average of three to five users. Table 8-1 shows the maximum number of users for a single MCU at each supported data rate. Figure 8-1 illustrates the service tables on a 3510 MCU. The maximum number of users in a single conference can reside in one or more conferences. Conferences at different rates can also reside on the same MCU and if there is not enough resources at the time of the call the call will be rejected.

Note: Continuous presence bandwidths are asymmetrical. A 384k four-user continuous presence call will actually consume 1.344M.

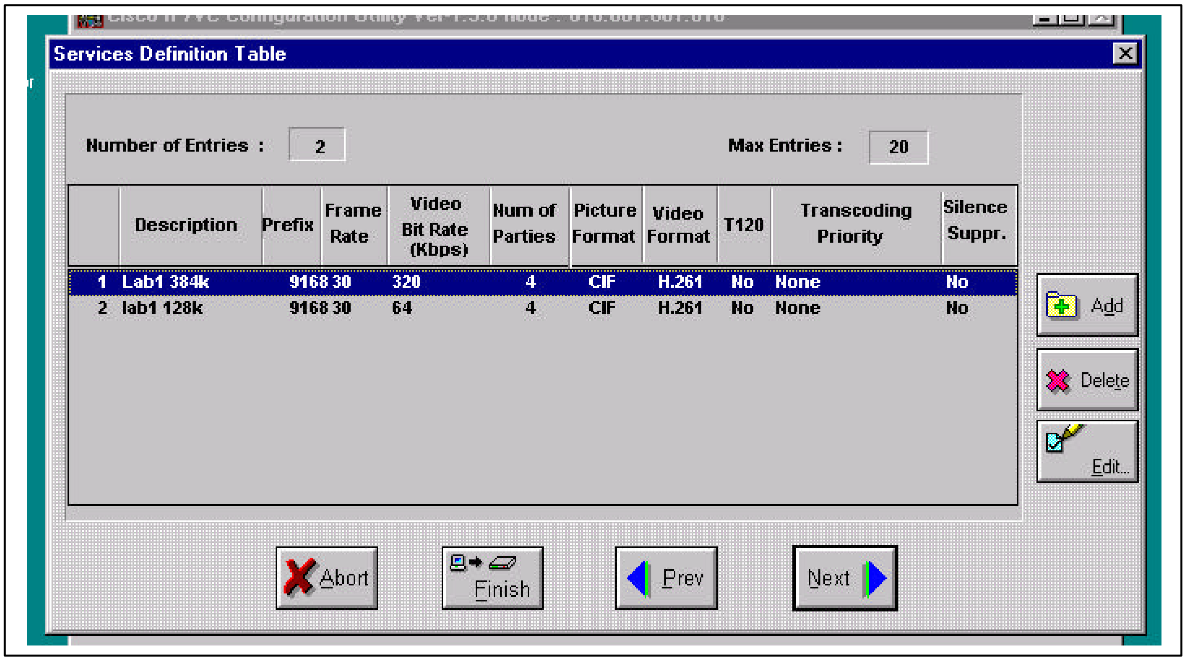
**Table 8-1**

| Data Rate | Maximum users |
|---|---|
| 128Kbps | 15 |
| 384Kbps | 9 |
| 512Kbps | 7 |
| 768Kbps | 5 |
| 1.5Mbps | 3 |

**Service Prefixes**:

| **Service Prefix** | Zone Prefix | E.164 Address |
|---|---|---|

## Figure 8-1



Cisco IP/VC Configuration Utility Ver 1.3.0 node : 010.001.001.010

Services Definition Table

Number of Entries : 2

Max Entries : 20

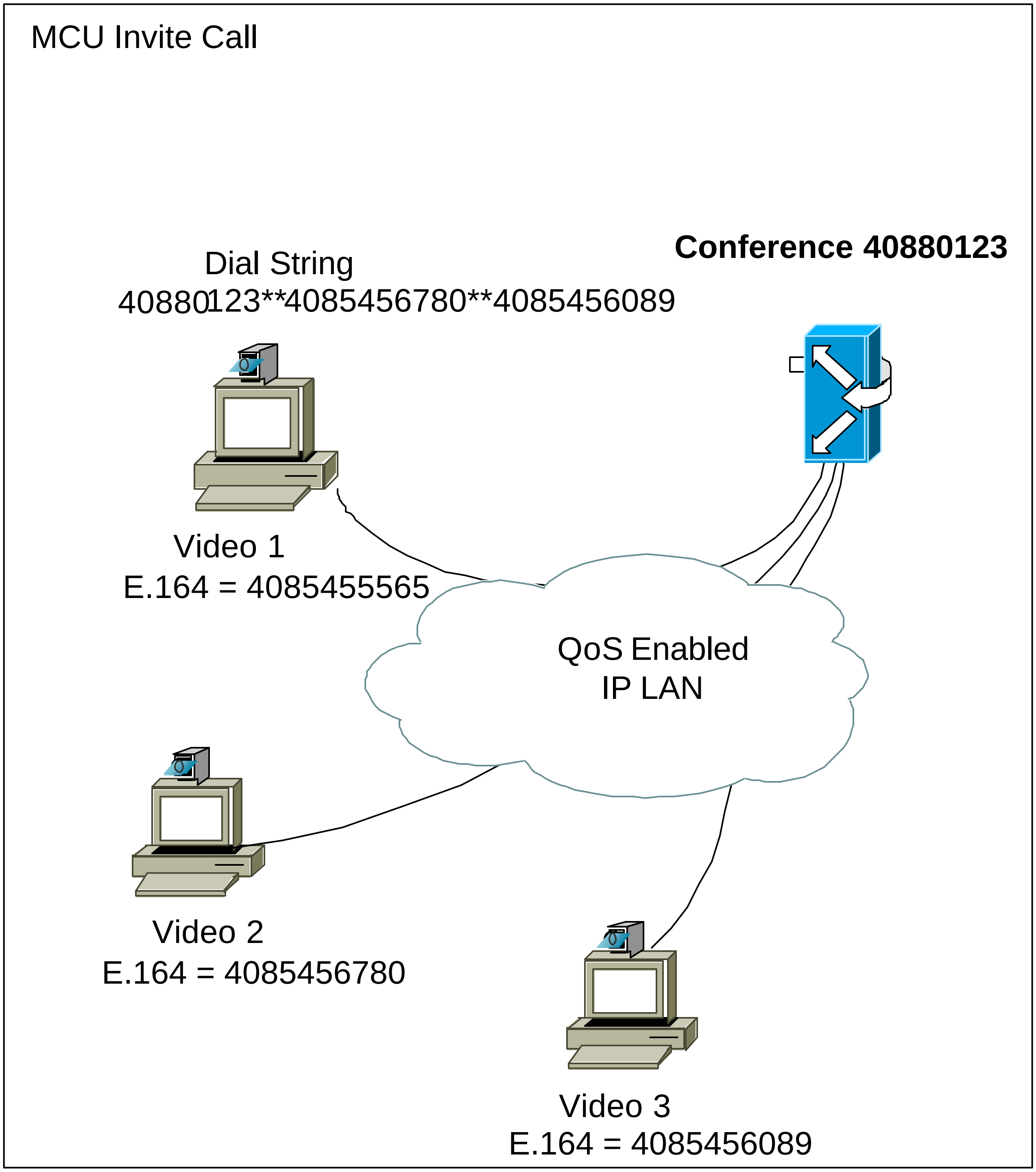
|  | Description | Prefix | Frame Rate | Video Bit Rate (Kbps) | Num of Parties | Picture Format | Video Format | T120 | Transcoding Priority | Silence Suppr. |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Lab1 384k | 9168 | 30 | 320 | 4 | CIF | H.261 | No | None | No |
| 2 | lab1 128k | 9168 | 30 | 64 | 4 | CIF | H.261 | No | None | No |

Add
Delete
Edit...
Abort
Finish
Prev
Next

## Initiating a call:

When an endpoint initiates a multipoint call they will dial the appropriate service prefix, followed by a conference ID (the conference ID can be up to 9 digits long).  If a service on an MCU is 40880 for a 384k call, the user might dial 4088011223, the call would be routed to the MCU using the 40880 service prefix, and the MCU would initiate an ad hoc conference with an ID of 4088011223.  Users can also initiate a call and invite the other participants by dialing the conference ID, invite string "**", and the E.164 address of the other participant.  Figure 8-2 shows the dial sequence of an MCU call with Video 1 initiating an MCU call to 40880123, and inviting Video 2 and Video 3.

**Figure 8-2**


MCU Invite Call
Dial String
40880123**4085456780**4085456089
Conference 40880123
Video 1
E.164 = 4085455565
QoS Enabled
IP LAN
Video 2
E.164 = 4085456780
Video 3
E.164 = 4085456089

MCUs can be configured to run as a single unit, in a stack, or single MCUs cascading conferences. Each of these configurations is discussed below.

## Single MCU:

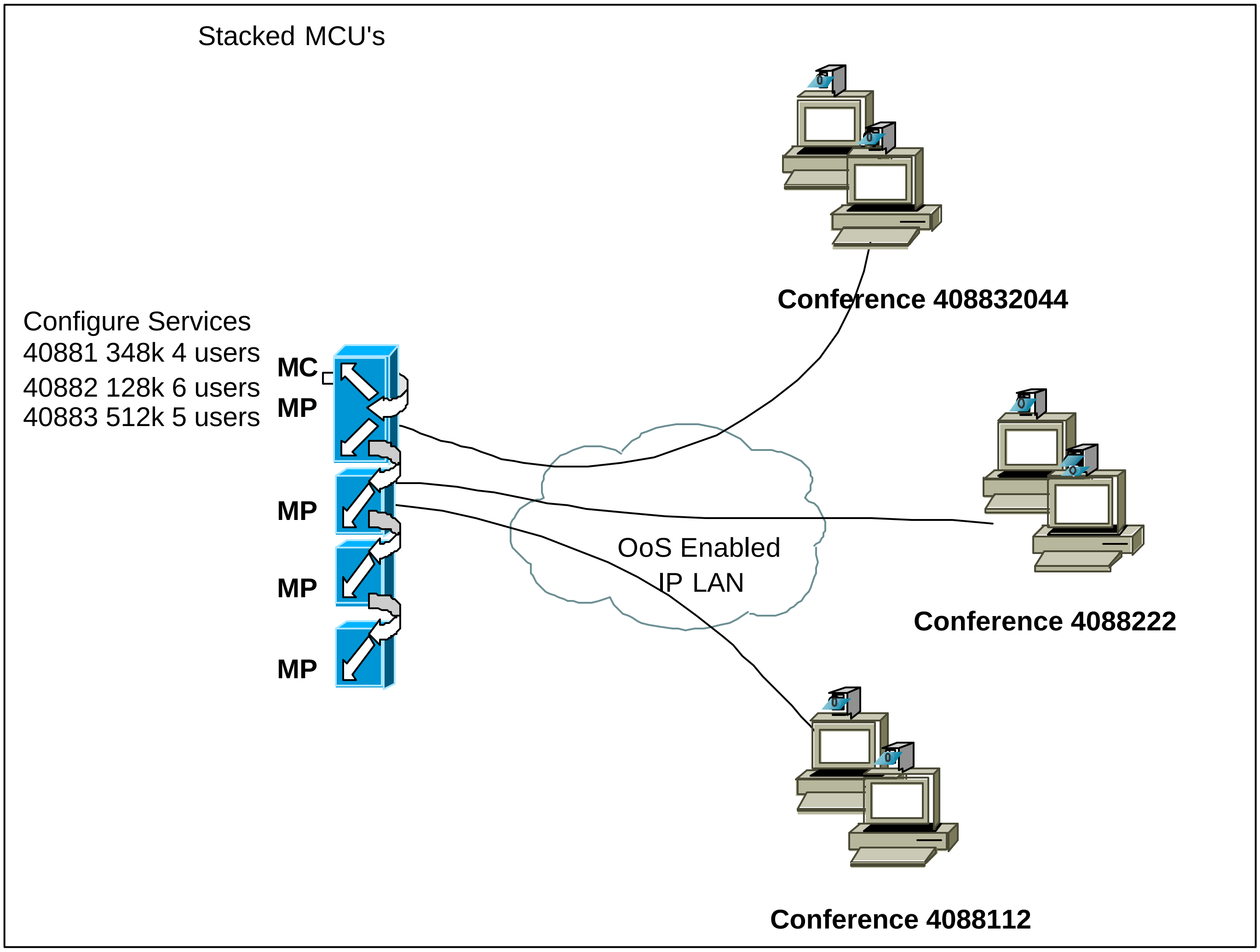
Configuring a single MCU allows the administrator to configure service prefixes that define conference settings on a single MCU. The MCU will be available for ad hoc conferences with the configured prefixes on a first come first server basis. A standalone MCU can also cascade conferences with another MCU(s) to create a larger conference (see cascading MCUs below).

## Stacking MCUs:

MCUs can be configured in a stack allowing managed services across multiple MCUs. Stacking MCUs allows the pooling of MCU resources; with up to four Multipoint processors (MP) being manage by one Multipoint controller (MC) (a stack usually consists of one MC/MP and up to three additional MPs). MCUs in a stacked environment are not physically connected together, but they will communicate over the LAN. The MC will manage all service prefixes and direct the media streams to the first MP with available resources. The MP performs the video processing and audio mixing for the conferences. Service prefixes will be defined only on the MC, which will distribute data streams among the configured MPs.

Figure 8-3 contains a single MC that is also configured as an MP and three additional MP's. The MC is configured with three service prefixes, 40881 – 384k, 40882 – 128k, and 40883- 512k that will be used to initiate multipoint calls on one or more of the MP's within the stack.

**Figure 8-3**

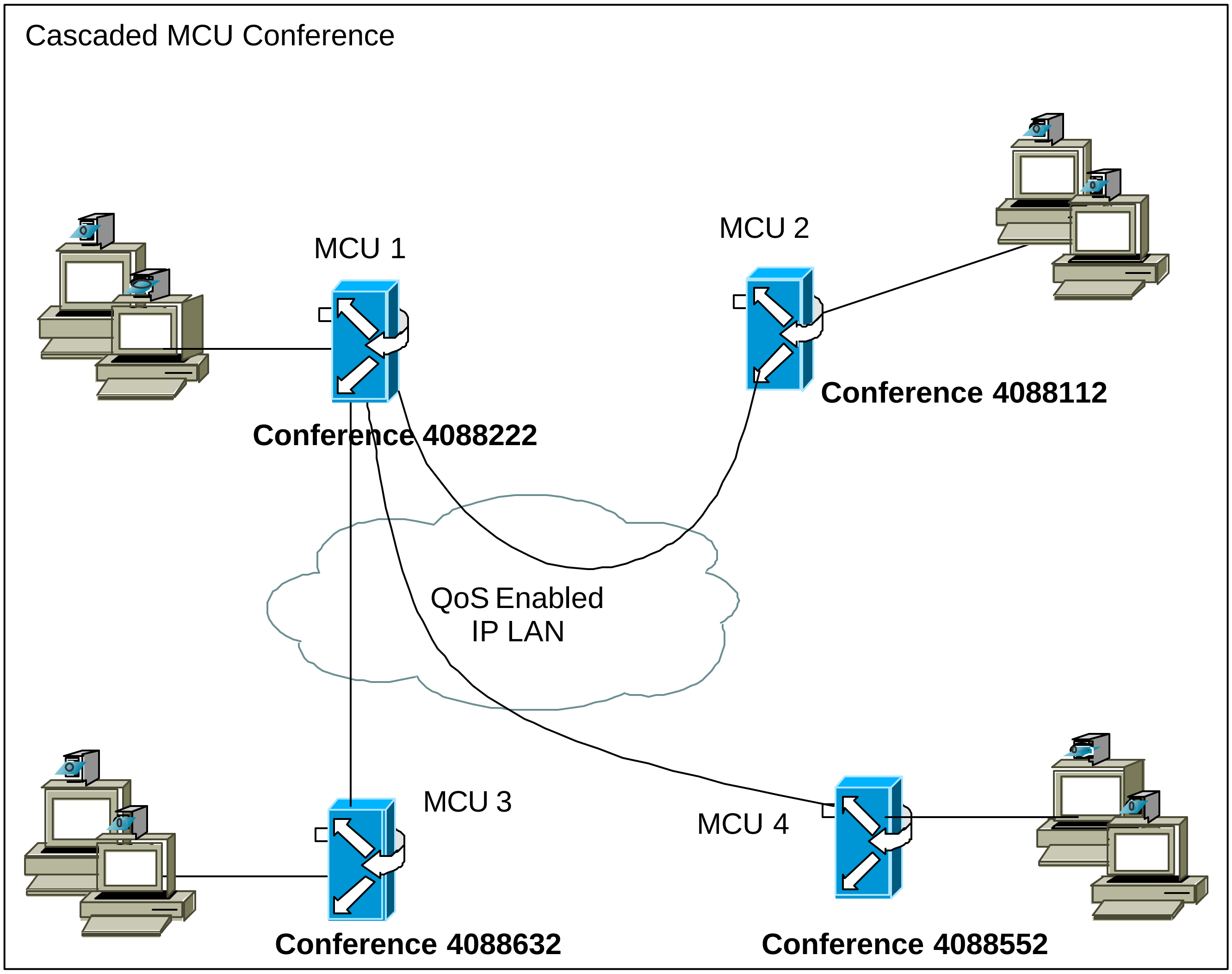


Note: A conference in a stack must reside on one MP, and cannot traverse multiple MPs in a stack. Stacking does not allow larger conferences, it will simply allow for more conferences using the same service prefix. This eliminates the need to have unique service prefixes for each of the MCUs. Conferences cannot exceed the capacity of a single MP in a stack Refer to table 8-1. Conferences will be initiated on the first MP with available resources in the stack. Also be aware creating a stacked MCU environment creates a single point of failure, if the MC is goes down the entire stack is lost. There are no physical connections made between stacked units. Connections are made over the LAN or WAN allowing MCUs to reside in the same location or across the WAN.

## Cascading MCUs:

The IP/VC 3510 MCU was designed for ad hoc conferences with an average of three to five users. In some instances, conferences will need to support more video terminals than one MCU can handle. MCU conferences can be cascaded to support larger conferences. Cascading MCUs is done by bringing conferences running on different MCUs together in a single joined call. In figure 8-4 a conference has been started on each of the four MCUs. To cascade the MCUs in this example, an administrator must access the web interface on MCU 1, and invite conferences 4088112 on MCU 2, 4088632 on MCU 3, and 4088552 on MCU 4.

## Figure 8-4



Note: There is no physical connection made between devices when cascading. Cascading occurs over the LAN or WAN allowing MCUs to be distributed across a network. MCUs can invite another H.323 endpoint, H.320 endpoint through a gateway, or another MCU through the web interface on the MCU.

**Distributed MCUs:**

With the ability to cascade multi point conferences administrators can build an H.323 video network with distributed MCU services. This saves WAN bandwidth when a conference must include multiple participants on two (or more) campuses connected by a WAN. By distributing MCUs across the network it is possible to have multi point conferences across WAN links, without limiting the number of users at remote sites. Centrally locating MCU services will require all conference participants to place a call across the WAN to the MCU. Distributing MCUs allows users to call to their local MCU, and the MCUs are then joined together into a cascaded conference across the WAN. Figure 8-5 illustrates centralized MCU services with three users from Campus B joining a conference hosted at Campus A. With this model all three calls must traverse the WAN link.

## Figure 8-5

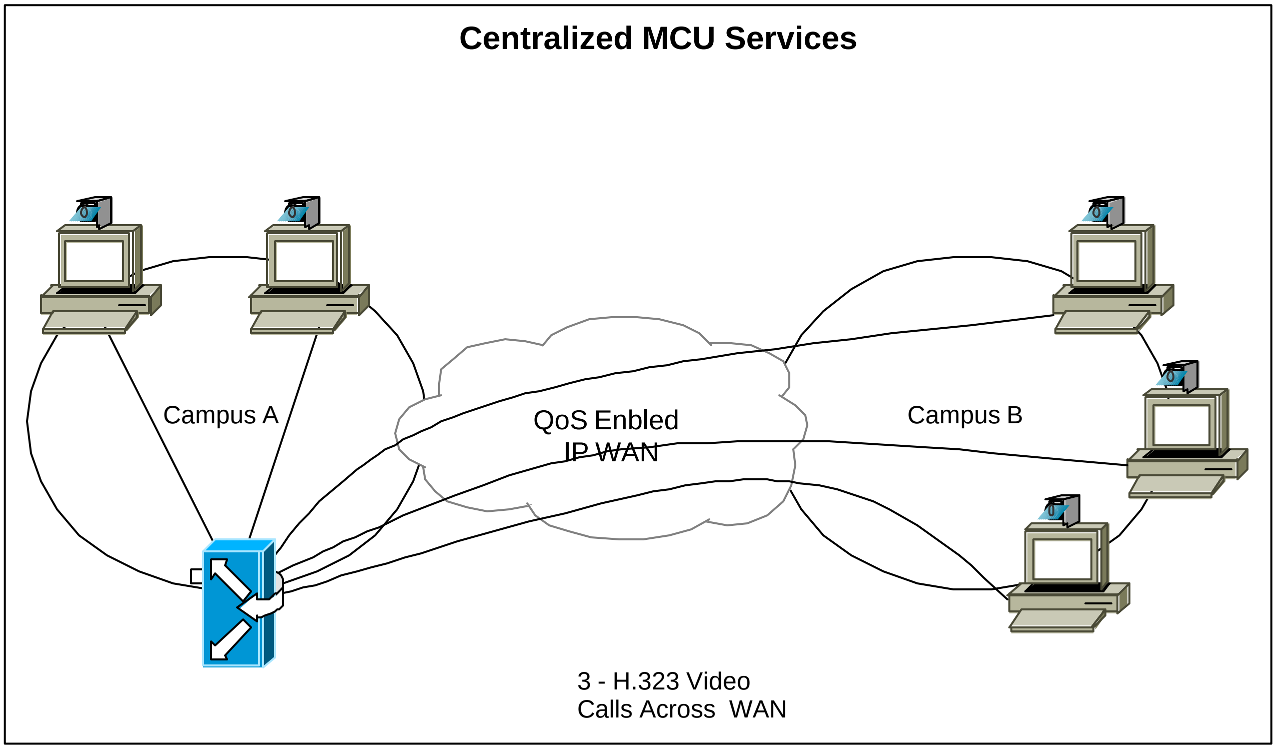
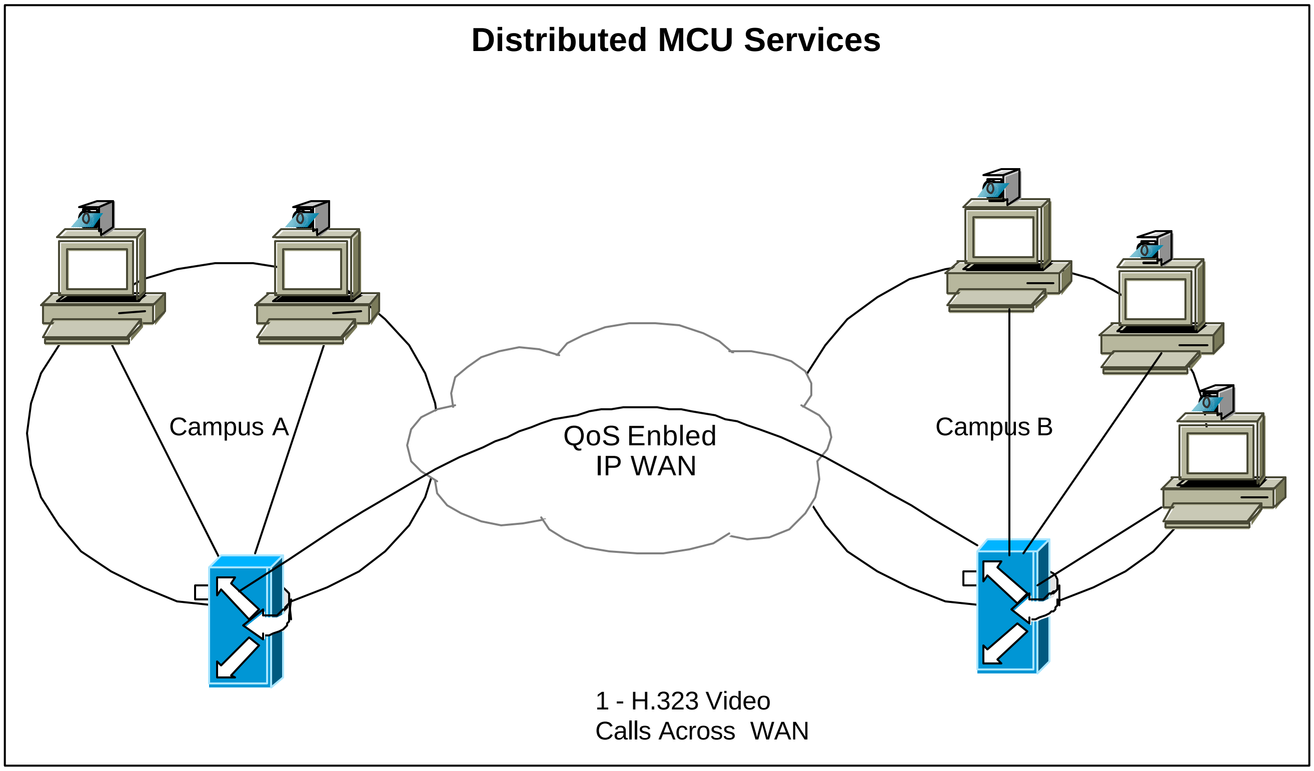


Figure 8-6 illustrates a distributed MCU model with two video terminals at Campus a calling into a local MCU, and three video terminals at Campus B calling into a local MCU, with a single call cascading the two conferences across the WAN.

## Figure 8-6



## Multipoint Conference Unit (MCU) 3540:

The Cisco IP/VC 3540 is a chassis based unit supporting MCU modules with a capacity of 100 128k video calls, dual PRI H.320 gateway modules, and T.120 Application server modules. The 3540 supports both voice activated and continuous presence calls. Each 3540 MCU blade supports a 10/100M Ethernet interface, supports H.261and H.263 video codecs, G.711, G.722 and G.728 voice codecs, and video data rates from 128kbps to 1.5Meg. Configuration of the MCU will depend on the desired function and network layout. The IP/VC 3540 was designed to support a large number of scheduled and ad hoc conferences. There are three MCU blades available for the 3540 MCU Table 8-2 lists the three modules and support number of calls at each data rate. The 3540 supports cascaded calls and can be used in conjunction with the IP/VC 3510 to create a distributed MCU architecture.

Note: Continuous presence bandwidths are asymmetrical. A 384k four-user continuous presence call will actually consume 1.344M.

**Table 8-2**

| Module | Data Rate | Maximum Users |
|---|---|---|
| 100 Session | 128k | 100 |
| | 384k | 50 |
| | 768k | 25 |
| | 1.5/2.0M | 10 |
| | Voice only | 150 |
| 60 Session | 128k | 60 |
| | 384k | 30 |
| | 768k | 15 |
| | 1.5/2.0M | 5 |
| | Voice only | 90 |
| 30 Session | 128k | 30 |
| | 384k | 15 |
| | 768k | 9 |
| | 1.5/2.0M | 3 |
| | Voice only | 45 |
| | | |

Note: the continuous-presence feature decreases the total number of participants supported by approximately 35 percent.

The Gateway blade (due out mid-2001) provides connectivity between ISDN-based H.320 participants and IP-based H.323 endpoints. The gateway module has a single 10/100 Ethernet interface, two Primary Rate Interface (PRI) ports that are configurable to T1 or E1 speeds, and support a wide range of switch protocols. It supports H.261 and H.263 video and G.711, G.722, and G.728 audio for optimum videoconference quality. The T.120 features of the module allow multimedia data conferences to take place among IP and ISDN users. The gateway supports conferences at bandwidths up to 384 kbps, and is available with optional audio transcoding capabilities.

The T.120 Application Server is a Pentium/NT server platform that hosts applications critical to multimedia conferences, including the T.120 Data Conferencing Server Application. The Application Server/Data Conferencing Server combination makes data sharing an integral part of multipoint conferences. PC-based H.323 endpoints can be equipped with a T.120 application that allows users to dynamically share views of an application such as spreadsheets or Web pages. The ability to interactively change numbers in an analysis, point to a Web-page feature, view diagrams, graphic presentations, or slide lectures, or engage in text chats, whiteboard exchanges, or rapid file transfers can all greatly enhance the discussion.

# Video Gateways:

The IP/VC 3520 and 3525 Videoconferencing Gateways give enterprises the ability to connect ISDN-based H.320 systems with IP-based H.323 videoconference endpoints. These gateways provide translation services between H.320 and H.323 networks to convert multimedia information between circuit-switched ISDN and IP networks. The gateway also supports G.711 and voice transcoding between IP and the PSTN. These systems enable users to videoconference with others via the LAN or the Public Switched Telephone Network (PSTN), regardless of location.

- The IP/VC 3520 Gateway is available in multiple configurations. The gateway can be configured with two or four BRI ports; two or four V.35 ports; or two BRI and two V.35 ports. When equipped with V.35 ports the IP/VC 3520 supports RS-366 or V.25bis signaling, allowing the gateway to set up circuit-switched connections through a DCE device such as an inverse multiplexer (IMUX) or access concentrator at speeds up to 768kbps. When the gateway is equipped with BRI ports the gateway will support bonded calls up to 384kbps.

- The IP/VC 3525 is a self-contained system that supports a high volume of calls over a single high-speed ISDN PRI connection. With the IP/VC 3525, multiple H.323 endpoints can share this PRI T1/E1 system when communicating with ISDN-based endpoints. This gateway can support up to eight sessions at 128kbps, or three at 384kbps (T1), four sessions at 384k (E1), or a mixture or the above. Sessions at different speeds may take place simultaneously.

The IP/VC 3520 has multiple configuration options allowing for flexible configuration of BRI or V.35. The PRI will support a single PRI allowing dynamic allocation of its 23 B channels. Table 8-3 shows the maximum numbers of calls supported per platform.

## Table 8-3

| | |
|---|---|
| IP/VC 3520 4 X BRI | |
| Call Data Rate | Maximum # of Calls |
| 128K | 4 |
| 384K | 1 |
| IP/VC 3520 4 X V.35 | |
| Call Data Rate | Maximum # of Calls |
| 128K* | 12 |
| 384K* | 4 |
| 768K** | 4 |
| IP/VC 3525 | |
| Call Data Rate | Maximum # of Calls |
| 128K | 8 |
| 384K | 3 for T-1, 4 for E-1 |

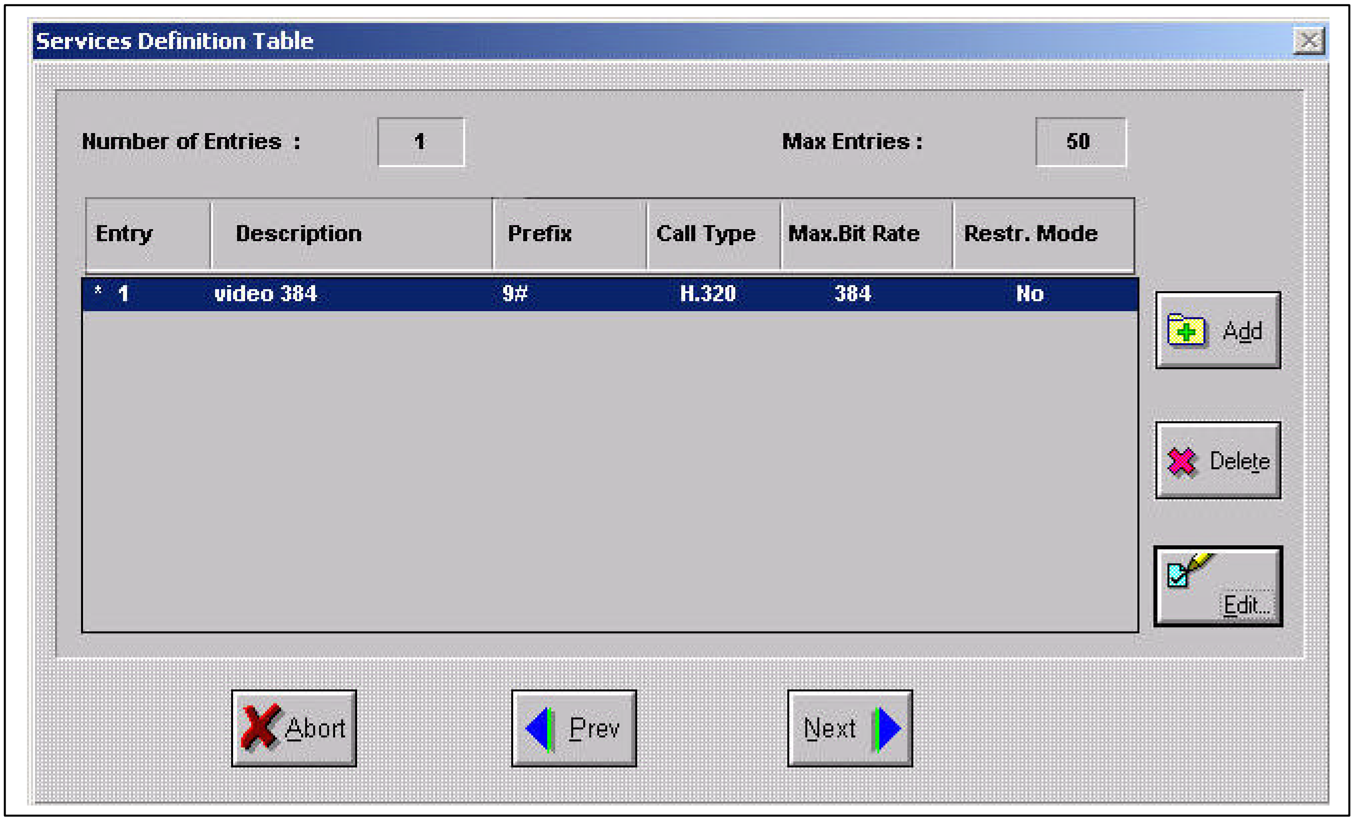
* Numbers based on an IMUX with three BRI lines
** Requires an IMUX with PRI connectivity or ISDN switch with a PRI connection

**Service Prefixes**

Video gateways must be configured with service prefixes to define the speed of outgoing calls, and routing of calls to the video gateway. In the voice world dialing 9 to gain an outside line is very common. In order to keep dialing strings consistent with existing voice dial plans it is suggested to use 90, 91 and so on for video gateway service prefixes. From the users perspective they will need to dial this service prefix, which in this case is equivalent to an access code, and the ISDN number of the H.320 video unit. In order to accomplish this a local (intra zone) gateway will be used whenever one is present. In zones that do not contain a gateway the administrator will assign a gateway in another zone as that zones primary gateway. Configuring LRQ forwarding or a static hopoff statement will route all calls to a zone with a gateway for PSTN access. Figure 8-7 illustrates the service prefixes for a PSTN gateway.

| | | |
|---|---|---|
| **Service Prefix** | Zone Prefix | E.164 Address |

## Figure 8-7



Services Definition Table

Number of Entries : 1

Max Entries : 50

| Entry | Description | Prefix | Call Type | Max.Bit Rate | Restr. Mode |
|---|---|---|---|---|---|
| * 1 | video 384 | 9# | H.320 | 384 | No |

Routing calls from the PSTN to H.323 endpoints can be done one of four ways. Each of the four methods are defined below and discussed in detail through out this document.

**MSN (Multiple Subscriber Numbering)**

Multiple Subscriber Numbering (MSN) is a group of phone numbers assigned to a particular ISDN line by the Telephone Company. MSN is not available in most regions of the U.S., Canada, or South America for BRI ISDN, but is widespread in Europe. Primary Rate (PRI) ISDN lines can be assigned multiple numbers in the U.S. and Europe; these are referred to as Direct Inward Dial (DID) numbers.

**IVR (Interactive Voice Response)**

IVR is a widely deployed automated call answering system that responds with a voice menu, allowing the H.320 endpoint to access H.323 endpoints by entering an extension from a keypad. When an incoming call arrives, the IVR answers the call, asks for the extension, the caller enters the E.164 address, and the call is transferred to the appropriate H.323 endpoint. Using IVR requires the calling H.320 endpoint to support DTMF. Most legacy room systems support DTMF.

**TCS4**

TCS4 is a special method for routing incoming H.320 video calls using extensions. TCS4 allows direct inward dialing to a H.323 endpoint on the LAN. H.323 endpoints on the LAN register to the gatekeeper with an E.164 number. When an H.320 endpoint dials a gateway's phone number followed by a TCS4 delimiter and the E.164 number, the call is routed directly to the corresponding H.323 endpoint. TCS4 is fairly new, and only some of the H.320 endpoints permit the user to enter a TCS4 extension when dialing. TCS4 is not used very often for incoming call routing, IVR is a better choice.

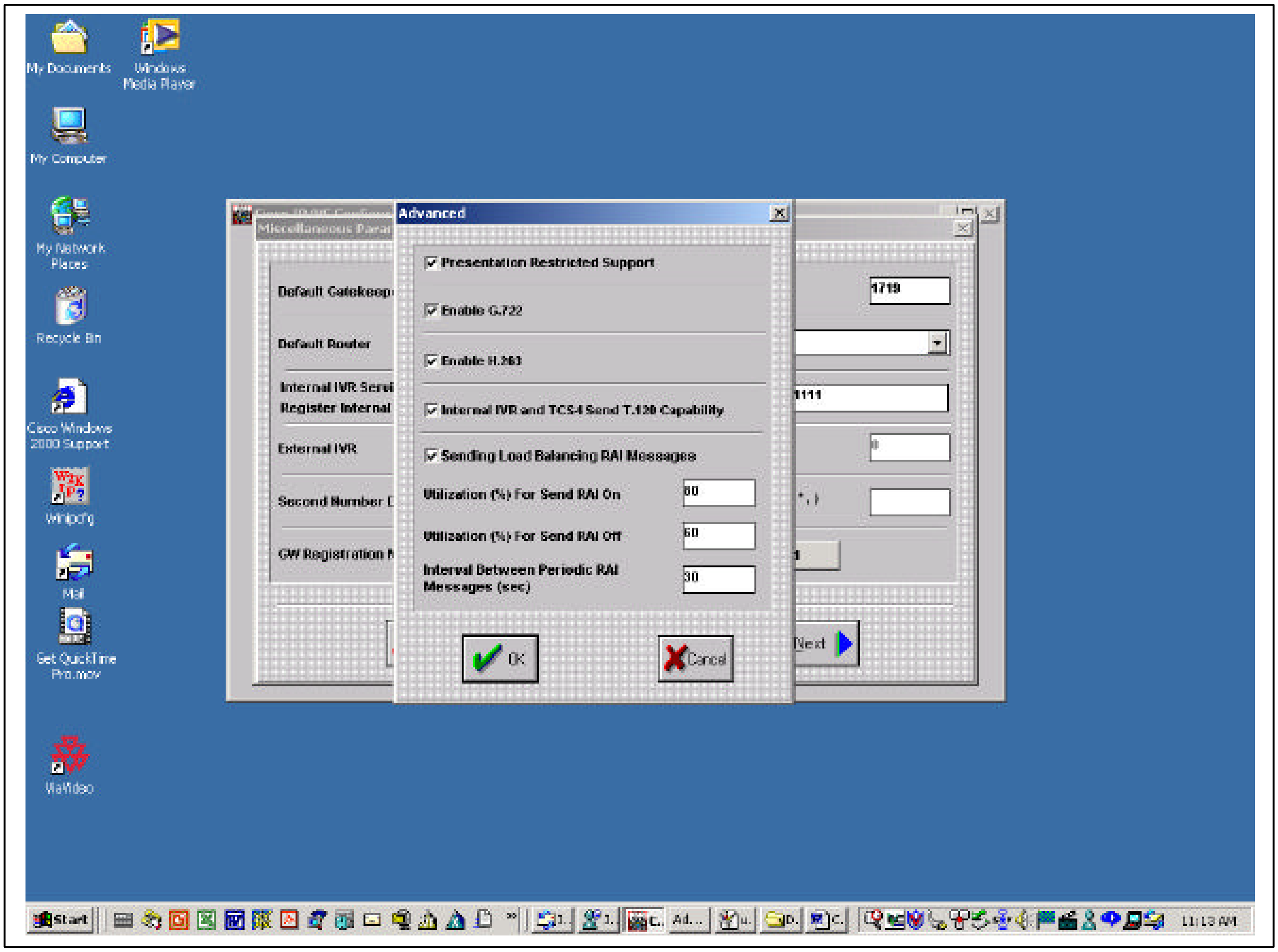
**Default Extension**

Entering a Default Extension in the gateway will force all calls received by the video gateway to be routed directly to a default E.164 address. Default Extension can also be used in conjunction with any of the routing methods mentioned above. If the call can't be routed by one of the above methods the call will then be forwarded to a default address.

## Line Hunting:

Out bound Line Hunting (LAN to PSTN) is a supported feature on the IP/VC 352X gateways. Line hunting allows users to build a pool of gateways for PSTN access. This creates a larger number of access lines serviced by a single set of service prefixes. With the current release of gateway code (ver. 2.2) for the IP/VC 3520 and 3525 Line hunting is support using Resource Availability Information (RAI) and Resource Availability Confirmation (RAC). Multiple gateways are configured with identical service prefixes and registered with the same gatekeeper. Outbound PSTN calls are sent to gateways based on resource availability using RAI and RAC. In the gateway configuration utilization parameters are set based on gateway resource percentages. Figure 8-8 shows the configuration screen from an IP/VC gateway. There are three configuration parameters: 1.) Utilization for sending RAI on, 2.) Utilization for sending RAI off, and 3.) Interval between periodic RAI messages. Sending a RAI on message instructs the gatekeeper that resources are running low and that calls should not be forwarded to the gateway (the default for sending a RAI on is 80%). Sending a RAI off message instructs the gateway that there is enough available resources and calls can be forwarded to the gateway (the default for sending a RAI off is 60%). Periodic RAI messages are sent from the gateway to the gatekeeper when one of the above thresholds is not achieved in a period of time (the default for these periodic messages is 30 seconds).

## Figure 8-8



Advanced

☑ Presentation Restricted Support

☑ Enable G.722

☑ Enable H.263

☑ Internal IVR and TCS4 Send T.120 Capability

☑ Sending Load Balancing RAI Messages

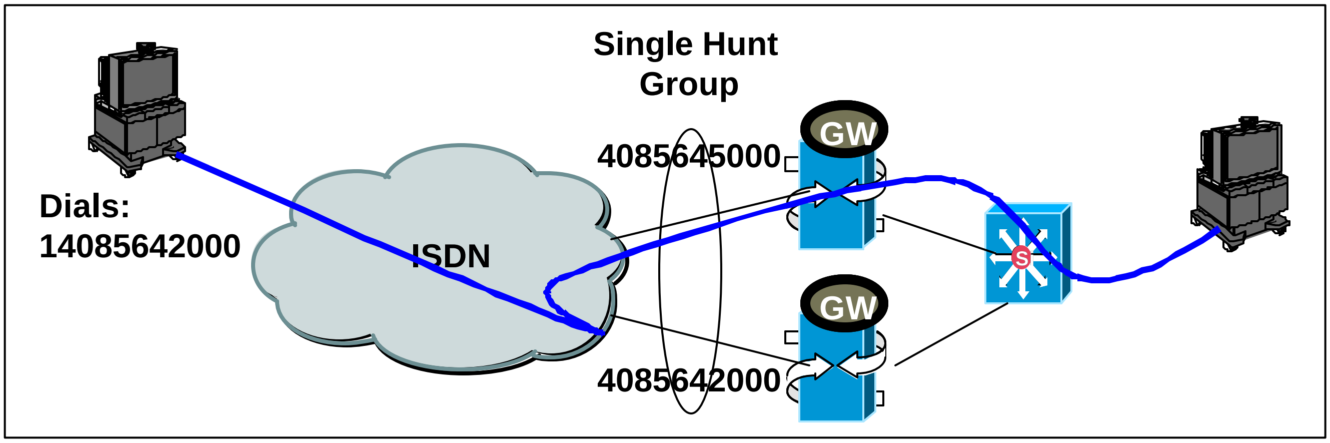
Utilization (%) For Send RAI On: 80

Utilization (%) For Send RAI Off: 60

Interval Between Periodic RAI Messages (sec): 30

Inbound line hunting (PSTN to LAN) can be done but is not very eloquent. Telcos are able to build hunt groups across multiple PRI lines allowing calls to be rolled to a second PRI if the first is busy. “Busy” is the key word in the last sentence, all B channels on a PRI must be busy for a call to roll to a second PRI. In the voice world this is not a problem since each voice call takes a single B channel, but in the video world calls can be placed at different data rates. If a 384k video call is received on the first of two PRI lines in a hunt group, and there are two available B channels the call will fail due to lack of resources. The only way inbound line hunting will work is to standardize on a data rate, say 384k, and busy out the odd number of channels. With 384k selected as the standard data rate five B channels would need to be busied out on each PRI. When three 384k calls are in progress on a PRI it will be completely busy, when three calls are in progress, and the Telco will route the next incoming call to an available PRI in the hunt group. If any user places a call at a data rate other than 384k in the example above this model breaks. Today this is as close as it gets to incoming line hunting. Figure 8-9 illustrates two PRI gateways in a single hunt group.

**Figure 8-9**

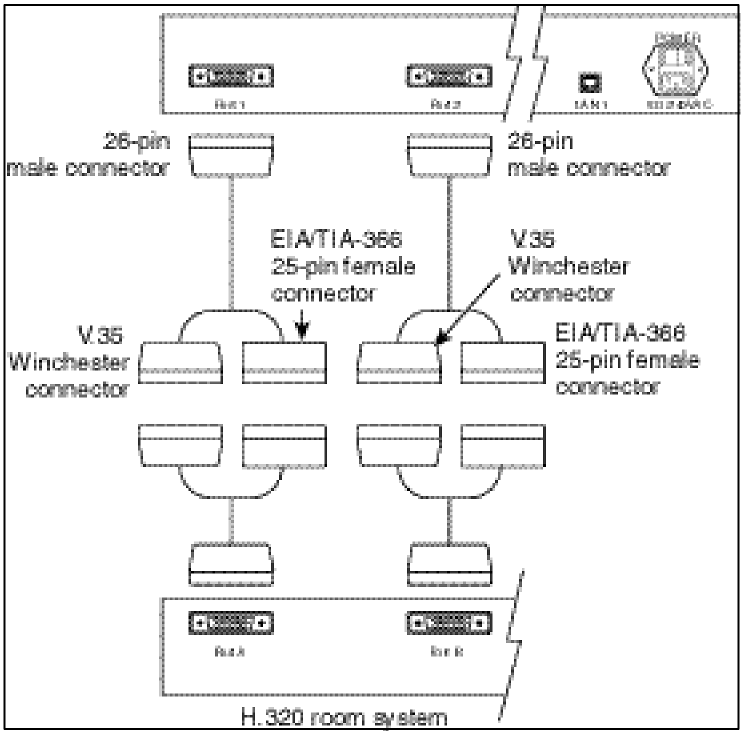


## Video Terminal Adapter:

The Video Terminal Adapter (VTA) IP/VC3530 allows customers to migrate existing H.320 video units from ISDN to an IP network. The VTA is a single port gateway that converts H.320 to H.323 for a single H.320 video terminal.

The VTA has two physical ports that connect directly to an H.320 codec. The supported connection from the VTA is V.35/RS-366 only, so if the H.320 codec doesn’t have V.35/RS-366 ports they will need to be added. Most H.320 codecs support this connection, but some H.320 systems may be installed with a different interface such as BRI or PRI. Even though there are two ports on the VTA only one H.320 codec can be attached to each VTA. If all calls made from an H.320 codec through a VTA are bonded calls, only one V.35/RS-366 connection is required. If 2 X 56 or 2 X 64kbps calls are going to be made both ports must be connected. Figure 8-10 illustrates the connection from a VTA to an H.320 codec.

**Figure 8-10**



Since the VTA is a gateway device and doesn't negotiate the call data rate automatically prefixes and suffixes must be added for different data rates. When the VTA is initially configured the administrator selects a default incoming and outgoing data rate. When calls are placed or received at the defined default data rate no prefix or suffix is needed. If a call is going to be placed or received at a speed other than the defined default data rate the prefix or suffix must be added.

To place a call at a data rate other than the default outgoing data rate the user must add a prefix to the dial string. Table 8-3 illustrates the prefix for each outgoing data rate. Remember when dialing the selected default the prefix does not need to be added by the user. When the prefix is added to the dialed number the VTA will see the #XX prefix, strip the prefix off of the number and place the call at the specified data rate.

### Table 8-3 Outgoing Call Prefixes:

| To Force Calling Bandwidth to: | Use Prefix: |
|---|---|
| 2 X 64 kbps (2B) | #00 |
| 128 kbps | #10 |
| 256 kbps | #20 |
| 384 kbps | #30 |
| 768 kbps | #70 |
| 2X56 kbps (2B restricted) | #01 |
| 112 kbps (restricted) | #11 |
| 224 kbps (restricted) | #21 |
| 336 kbps (restricted) | #31 |
| 672 kbps (restricted) | #71 |

Receiving calls at a data rate other than the specified default incoming data rate requires a suffix be added to the dial string. When the VTA is configured, a default incoming speed will be entered, and when receiving a call with no suffix that data rate will be used. When the VTA registers with the gatekeeper it will actually register with six E.164 addresses. If the E.164 address of a VTA were configured as 408565212 the VTA would register with the E.164 addresses listed in table 8-4.

### Table 8-4 Incoming Call Data Rates:

| E.164 Address | Supported Data Rate |
|---|---|
| 408565212 | Default Data Rate |
| 40856521200 | 2 X 64 kbps |
| 40856521211 | 128 kbps |
| 40856521220 | 256 kbps |
| 40856521230 | 384 kbps |
| 40856521270 | 768 kbps |
| 40856521201 | 2 X 56 kbps (restricted) |
| 40856521211 | 112 kbps (restricted) |
| 40856521221 | 224 kbps (restricted) |
| 140565621231 | 336 kbps (restricted) |
| 40856521271 | 672 kbps (restricted) |

# Multimedia Conference Manager (MCM):

The Multimedia Conference Manager (MCM) is an IOS software component that supplies gatekeeper and proxy functions for an H.323 video network. The IOS based gatekeeper allows large H.323 video networks to be built and managed on Cisco hardware. The proxy supplies needed functions that are not currently supplied by devices in some IP networks. Functions such as QoS, access to NAT networks, and firewall access are some of the functions that the proxy supplies.

## Gatekeeper:

The Cisco gatekeeper performs all call routing and address registration (RAS) for all H.323 video components. The gatekeeper is one of the most important components in an H.323 network. The gatekeeper is the central management device for an H.323 video network and performs functions required for a successful H.323 video deployment. Below are some of the most commonly used functions of the Cisco IOS Gatekeeper:

- H.323 component registration and call routing:
  The gatekeeper registers all video infrastructure components IP address, E.164 address, H.323-ID, device type, and signaling ports. This registration allows the gatekeeper to provide call routing for all devices that are registered with the gatekeeper.

- Bandwidth management:

  The Cisco gatekeeper can be configured to manage the bandwidth in a zone, between zones, or on a per call basis. Managing video bandwidth on IP networks is an essential feature of any gatekeeper.
  - Interzone: Total bandwidth allowed from a local or default zone to and from all other zones
  - Remote: Total bandwidth allowed from all local zones to and from all remote zones
  - Session: Bandwidth allowed per session in a zone
  - Total: Total bandwidth allowed in a zone

- AAA (Authentication, Authorization and Accounting) support
  The Cisco gatekeeper works in conjunction with RADIUS and TACACS servers to provide authentication of devices and accounting via call detail records (CDR).

The Cisco gatekeeper is supported on various router platforms, the supported platforms and performance data is listed below in Table 8-5.

## Table 8-5

| Chassis | IP Routing | H.323 Endpoint Registration | Simultaneous Video Calls | Video Proxy Sessions |
|---|---|---|---|---|
| 72XX | 50-100K pps | 3000 | 500 | 50 @ 768kbps<br>75 @ 384kbps<br>100 @ 128kbps |
| 3660 | 25-100K pps | 1800 | 250 | 25 @ 768kbps<br>35 @ 384kbps<br>50 @ 128kbps |
| 3640 | 10-40K pps | 1800 | 150 | 10 @ 768kbps<br>15 @ 384kbps<br>30 @ 128kbps |
| 3620 | 10-15K pps | 1800 | 75 | 10 @ 768kbps<br>15 @ 384kbps<br>30 @ 128kbps |
| 262X | 5-10K pps | 900 | 60 | 2 @ 768kbps<br>4 @ 384kbps<br>8 @ 128kbps |
| 261X | 2-5K pps | 900 | 60 | 2 @ 768kbps<br>4 @ 384kbps<br>6 @ 128kbps |
| 3810 | 2-5K pps | 900 | 60 | 2 @ 768kbps<br>4 @ 384kbps<br>6 @ 128kbps |
| 25XX | N/A | 600 | 30 | 2 @768kbps<br>4 @ 384kbps<br>10 @ 128kbps |

The Cisco gatekeeper also supports features that enable users to build reliable and scaleable networks. Two of the features that allow H.323 networks to scale are listed below.

- Hot Standby Router Protocol (HSRP) allows administrators to build a standby gatekeeper that will become active in event of a gatekeeper failure.
- Directory Gatekeeper or Location Request (LRQ) forwarding allows administrators to build large multi-tier networks, minimizing the configuration required in the lower-tier Gatekeepers. When a call is made in a lower-tier zone and a match is not found the call is automatically forwarded up to the directory gatekeeper for resolution. See Directory Gatekeeper in Chapter 7 for more information. Figure 8-11 illustrates a network configure with directory gatekeeper.

## HSRP:

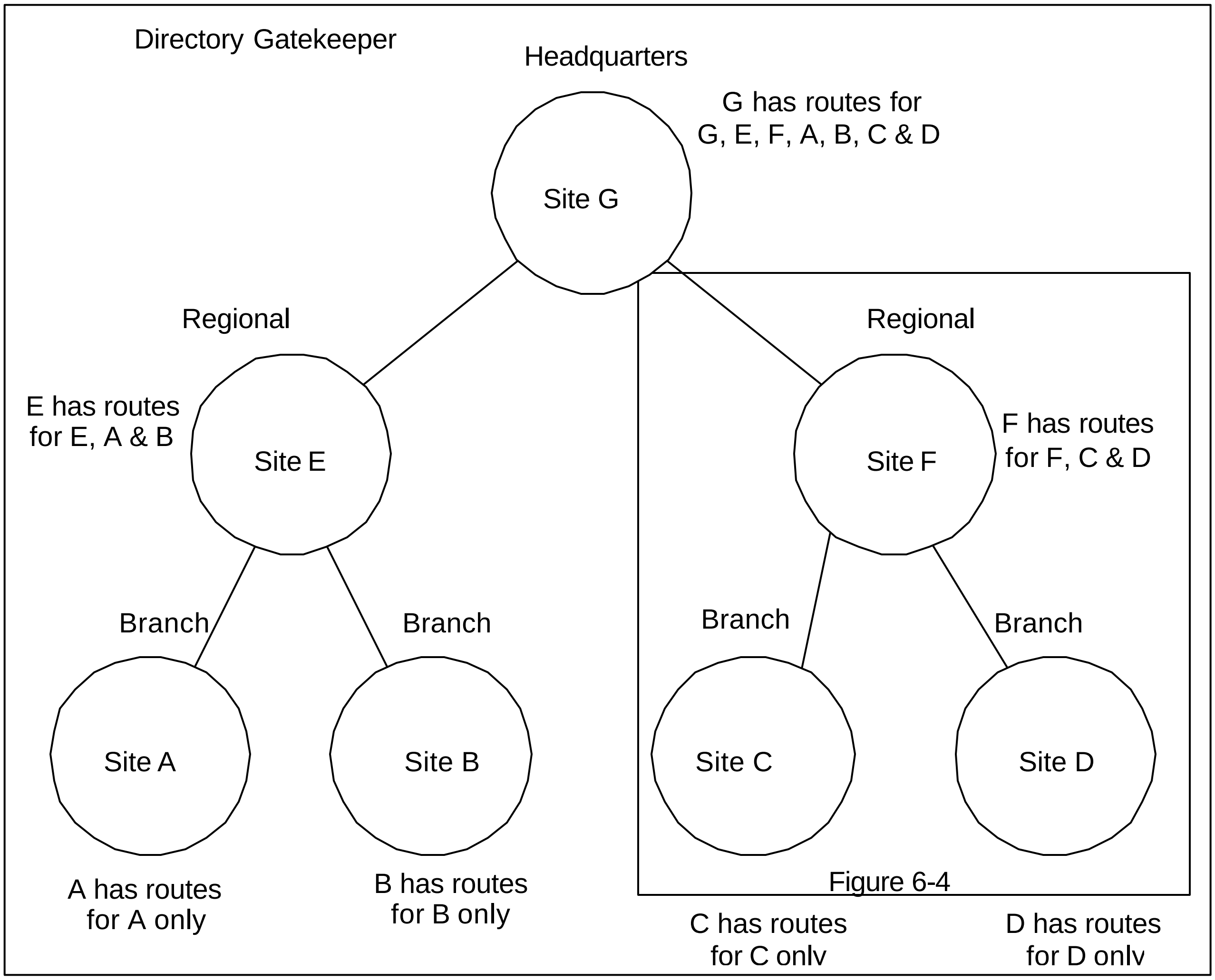
HSRP enables a set of routers with MCM to work together to present the appearance of a single virtual gatekeeper. This is accomplished by creating a "phantom" router that has its own IP and MAC addresses.

Based on the priority given by the network administrator, one of the HSRP routers/gatekeepers in each group is selected to be the active forwarder and the other to be a stand-by router/gatekeeper. The router/gatekeeper with the highest priority will act as the active router/gatekeeper. The active router does the work for the HSRP phantom. If an end node sends a packet to the phantom's MAC address, the active router/gatekeeper receives that packet and processes it. If an end node sends an ARP request for the phantom's IP address, the active router/gatekeeper replies with the phantom's MAC address.

The HSRP-configured routers/gatekeepers (both active and stand-by) watch for hello packets to monitor the status of each other. The router/gatekeeper group will learn the hello and hold timers as well as the standby address to be shared from the active router/gatekeeper. If the active router becomes unavailable for any reasons such as power failure, scheduled maintenance or misses responding to three successive hello packets, then the stand-by router will assume this functionality transparently within a few seconds. Because the new active router/gatekeeper assumes both the IP and MAC addresses of the phantom, video terminals registrations will time out and register with the same IP address on the now active router/gatekeeper.

Note: When configuring gatekeepers and proxies on routers supporting HSRP it is important that the configured proxies be configured to register with the “virtual” IP address of the gatekeeper pair. Both proxies will register with the active gatekeeper and video calls will be load balanced between the two proxies. If the primary router fails the proxy on the stand-by router will register with the now active “stand-by” gatekeeper, and calls will be forward through the single proxy. The proxy configured on the primary router will not reregister with the stand-by router if the primary router fails.

**Figure 8-11**


Directory Gatekeeper
Headquarters
G has routes for
G, E, F, A, B, C & D
Site G
Regional
Regional
E has routes
for E, A & B
Site E
Site F
F has routes
for F, C & D
Branch
Branch
Branch
Branch
Site A
Site B
Site C
Site D
A has routes
for A only
B has routes
for B only
Figure 6-4
C has routes
for C onlv
D has routes
for D onlv

## Proxy:

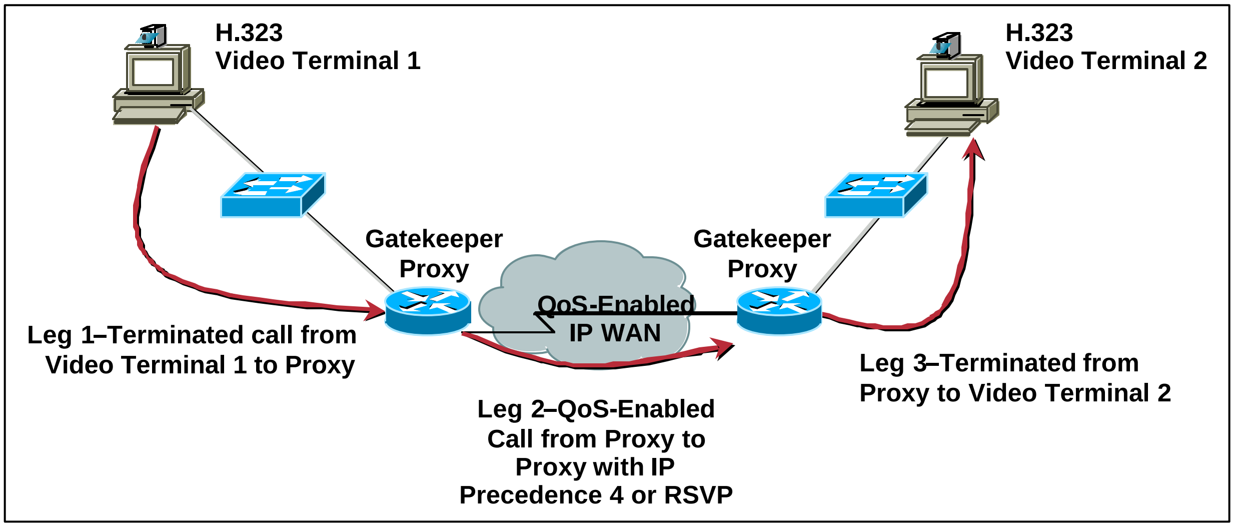
The MCM also provides a proxy, which functions as a call-processing agent to terminate H.323 calls from one local LAN or “zone” and establishes sessions with H.323 terminals located in different LANs or “zones”. The proxy provides the feature listed below.

- Classification of video/audio streams with IP Precedence or RSVP for QoS.
- Application Specific Routing (ASR), routing of Videoconference traffic to specific network links reserved for video traffic only.
- Allows access through Firewalls and NAT environments.

## Proxy QoS:

The Cisco proxy allows video terminals with no IP QoS capabilities to obtain traffic classification across WAN links. The proxy is configured to support RSVP or IP Precedence and registers with the local gatekeeper as an H.323 endpoint. The proxy is then used to classify traffic across low speed WAN links with the configured traffic classification. Each proxied call contains three call legs: one from the calling video terminal to the proxy registered in its zone, one from proxy to proxy across the WAN, and one from the remote proxy to the receiving video terminal. Figure 8-12 illustrates a proxied call across a WAN link.

## Figure 8-12

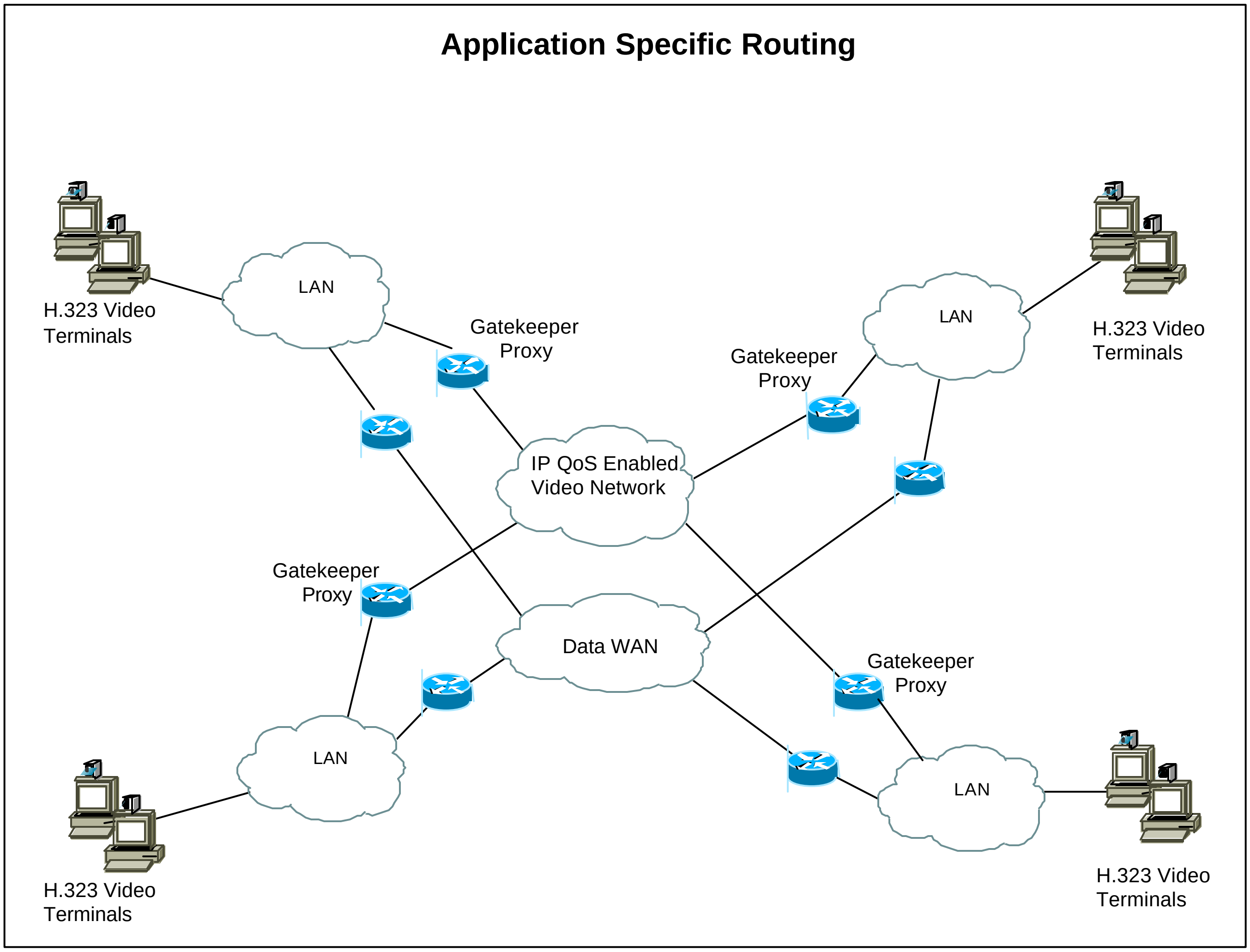


Note: Currently single legged proxy is supported in 12.1X, but there is a bug in the code that makes this configuration unusable. All video calls are only processed at 64k regardless of the call data rate.

## Application Specific Routing: (ASR)

In some cases administrators may want to separate real time video traffic onto a separate network that can guarantee bandwidth and delay. The proxy has the ability to route H.323 video traffic to specific router interfaces, allowing a separate video network to be built in parallel with the customer's data network. All proxies in the video network must be configured with the same traffic classifications, and the administrator must ensure that no data traffic has access to the video network. ASR requires a multi zone configuration with a proxy configured at each location. Currently all serial, Ethernet and Fast Ethernet interfaces support ASR. Figure 8-13 illustrates a network configured for ASR.

**Figure 8-13**



# Chapter 9:

# WAN Multi Zone Case Study:

This section will give you an example of a typical WAN multi zone model deployed in an enterprise WAN environment.

This Chapter contains the following sections:

- Overview
- Network Layout
- Network Design
- Dial Plan
- Video Infrastructure

## Overview:

In this case study the customer is a health care provider with locations spread across the United States. There are five locations that are currently using ISDN based videoconference. The customer has a T1 to each site and would like to install new H.323 videoconferencing units and utilize their existing WAN bandwidth. Each site contains a minimum of three video units and the customer has standardized on 384k as their call data rate. The customer requires multipoint calls as well as the ability to call off net to their customers.

## Network Layout:

Currently the customer has five sites in the United States consisting of Sacramento CA, Los Angeles CA, Dallas TX, Columbus OH, and Chicago IL. Each site is connect back to Columbus OH with a T1 and bandwidth utilization on all of the connections is fairly low. The customer has just upgraded their WAN routers at remote sites to 3640's to support voice video and data in the near future. Currently all videoconferencing units are directly connected to an IMUX with three BRI lines allowing boded 384k calls. The Columbus site contains an H.320 multipoint conference unit (MCU) with three PRI lines supporting multipoint calls among the sites. Figure 9-1 illustrates the customers IP network and Figure 9-2 illustrates the customer's current videoconferencing network.

**Figure 9-1**

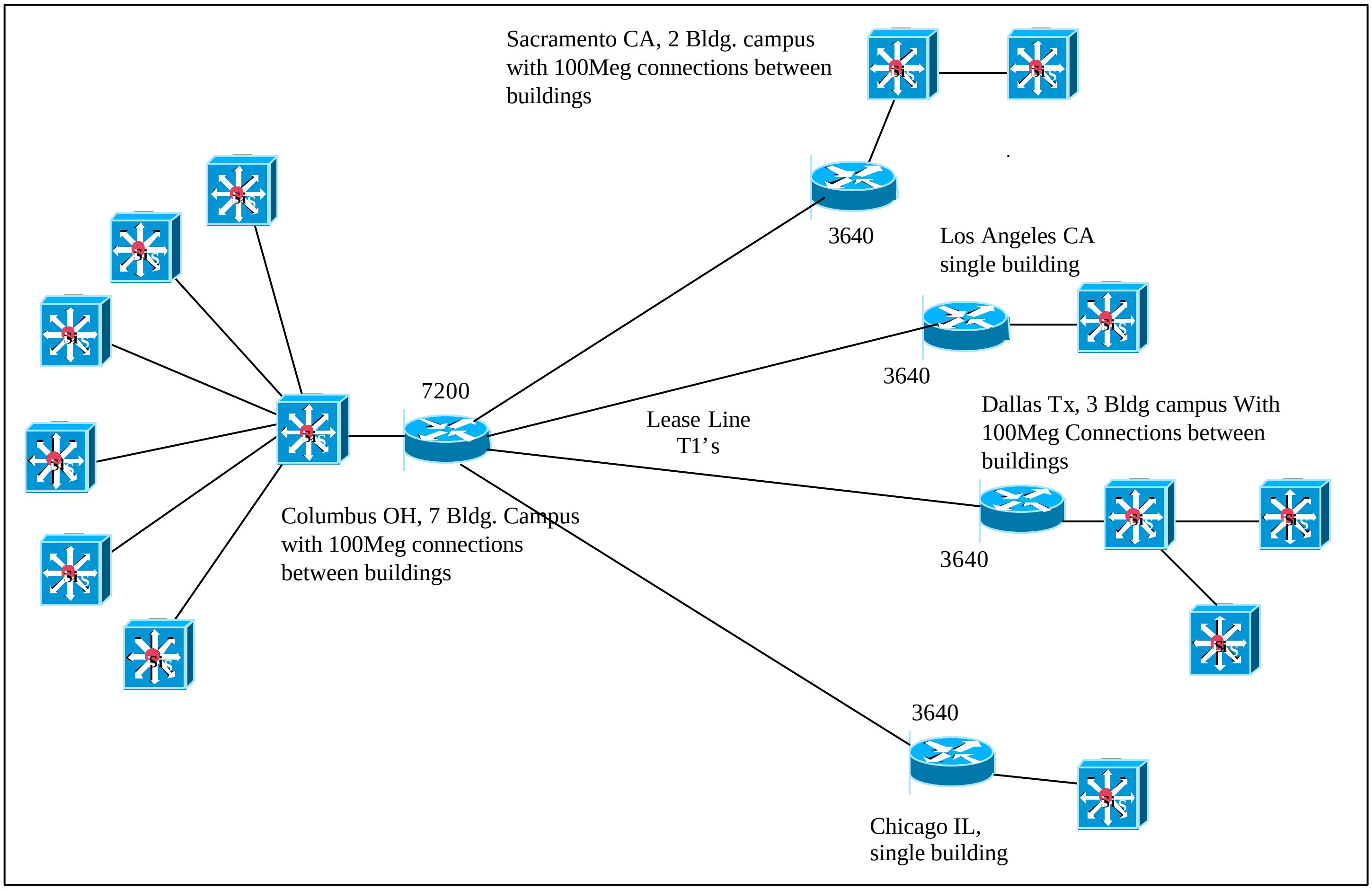
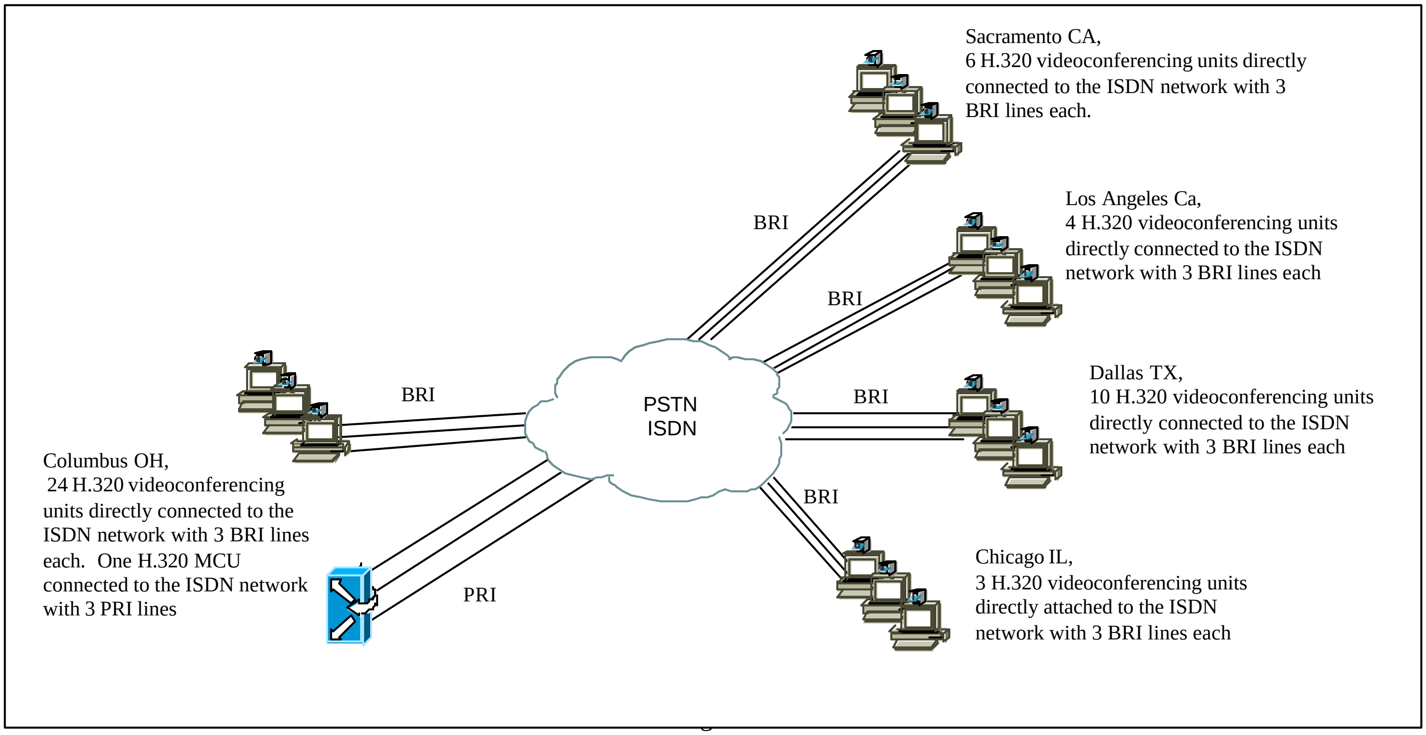

Sacramento CA, 2 Bldg. campus with 100Meg connections between buildings
3640
Los Angeles CA single building
7200
3640
Lease Line T1's
Dallas Tx, 3 Bldg campus With 100Meg Connections between buildings
Columbus OH, 7 Bldg. Campus with 100Meg connections between buildings
3640
3640
Chicago IL, single building

**Figure 9-2**


Sacramento CA, 6 H.320 videoconferencing units directly connected to the ISDN network with 3 BRI lines each.
BRI
Los Angeles Ca, 4 H.320 videoconferencing units directly connected to the ISDN network with 3 BRI lines each
BRI
BRI
PSTN ISDN
BRI
Dallas TX, 10 H.320 videoconferencing units directly connected to the ISDN network with 3 BRI lines each
Columbus OH, 24 H.320 videoconferencing units directly connected to the ISDN network with 3 BRI lines each. One H.320 MCU connected to the ISDN network with 3 PRI lines
BRI
PRI
Chicago IL, 3 H.320 videoconferencing units directly attached to the ISDN network with 3 BRI lines each

# Network Design:

The network outlined above is a classic WAN multi zone model, there is sufficient WAN bandwidth and each site contains three or more video terminals. In this network a gatekeeper and proxy will be located at each site. Directory gatekeeper services will be configured and HSRP will be used for gatekeeper redundancy at the Columbus site. There are two key elements that will need to be configured in the network to ensure video quality.

- Quality of Service
- Call Admission Control

## Quality of Service (QoS)

End to end QoS is a key factor to a successful deployment. The customer has decided to go with an H.323 video terminal that supports marking of IP Precedence. Columbus, Sacramento and Dallas have just upgraded their switches to Catalyst 6500's. In these two sites LAN QoS will be configured, the other three sites will support LAN QoS when the switches at those sites are upgraded. All video units will be connected to 10/100 Ethernet ports.

All video terminals will be configured to mark IP Precedence 4. In Columbus, Sacramento and Dallas trust boundaries will be set on the Catalyst 6500 switches. Video gateways and MCUs will also be installed in Columbus, Sacramento and Dallas. At this time gateways and MCUs don't support IP Precedence. IP Precedence will be marked and a trust boundary will be set on the Catalyst 6500 ports that the gateways and MCUs are connected to. Gateways will also be installed in Los Angeles and Chicago.

Priority queues will be configured on all WAN routers and be provisioned for 920k. This will guarantee that bandwidth is available for two 384k calls. An access list entry will also be added on the WAN router setting the entrance criterion for the priority queue. Only video traffic received from the proxy will be admitted to the priority queue.

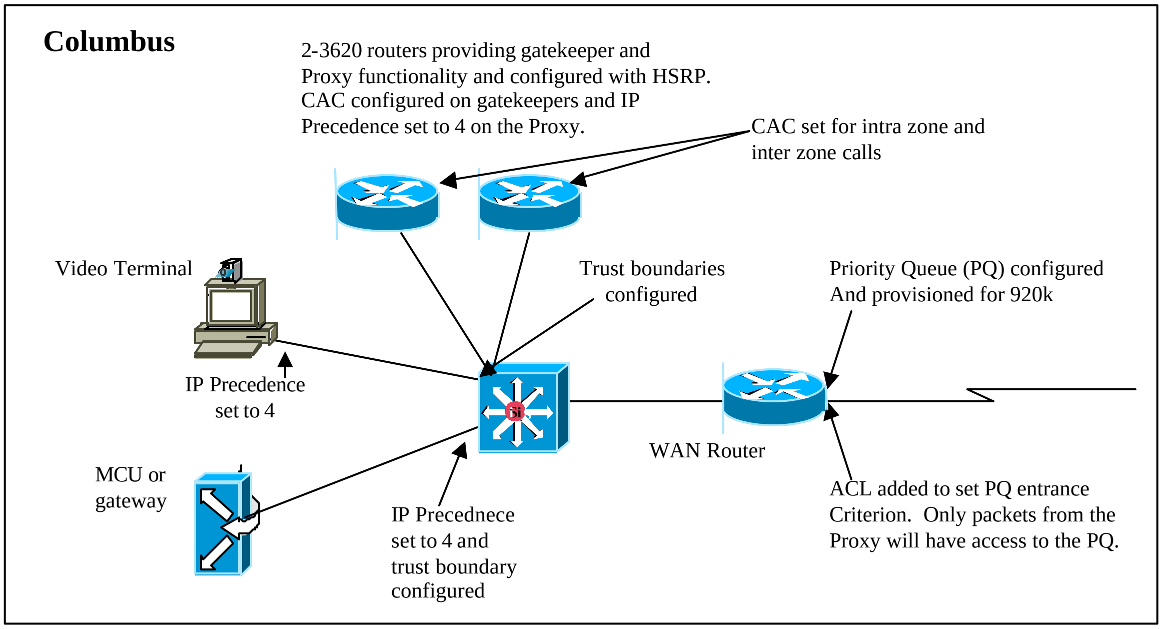
The gatekeeper at each site will be configured to use the local proxy for all inter zone calls. The proxy will rewrite IP Precedence 4 and provide a single access point to the configured priority queue.

For more information regarding network QoS refer to the AVVID QoS design guide at.
http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/avvidqos/index.htm

## Call Admission Control

Call admission control (CAC) must be implemented for inter zone calls. It is also a good idea to configure CAC for intra zone calls. Setting CAC on for inter zone calls guarantees that the provisioning on the priority queues will not be exceeded. If the provisioned bandwidth for the priority queue on the WAN route is exceeded all video calls in the queue will be effected. The gatekeeper at each site will contain three bandwidth statements for CAC. 1.) bandwidth total default <bandwidth> 2.) bandwidth remote 1536 3.) bandwidth session default 768. It is important to note that the bandwidth is calculated in half duplex, so the call data rate must be doubled. A 384k call is represented as 768 in the bandwidth statements. With the three-bandwidth statements above we have limited the total bandwidth in the local zone (to a number yet to be decided). Limited the remote bandwidth (available bandwidth to and from any remote zone) to 1536, or two 384k calls. The bandwidth per session has been limited to 768 or 384k. Figure 9-3 illustrates QoS and CAC points for Columbus, Figure 9-4 illustrates QoS and CAC points for Dallas and Sacramento and 9-5 illustrates QoS and CAC points for Los Angeles and Chicago.

## Figure 9-3


Columbus
2-3620 routers providing gatekeeper and
Proxy functionality and configured with HSRP.
CAC configured on gatekeepers and IP
Precedence set to 4 on the Proxy.
CAC set for intra zone and
inter zone calls
Video Terminal
Trust boundaries
configured
Priority Queue (PQ) configured
And provisioned for 920k
IP Precedence
set to 4
WAN Router
MCU or
gateway
IP Precednece
set to 4 and
trust boundary
configured
ACL added to set PQ entrance
Criterion. Only packets from the
Proxy will have access to the PQ.

## Figure 9-4

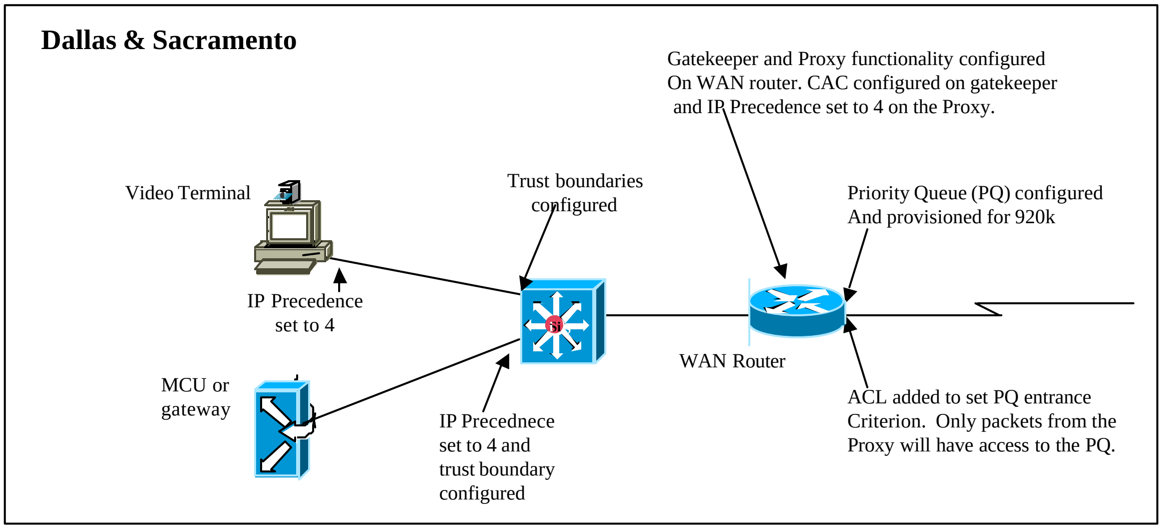
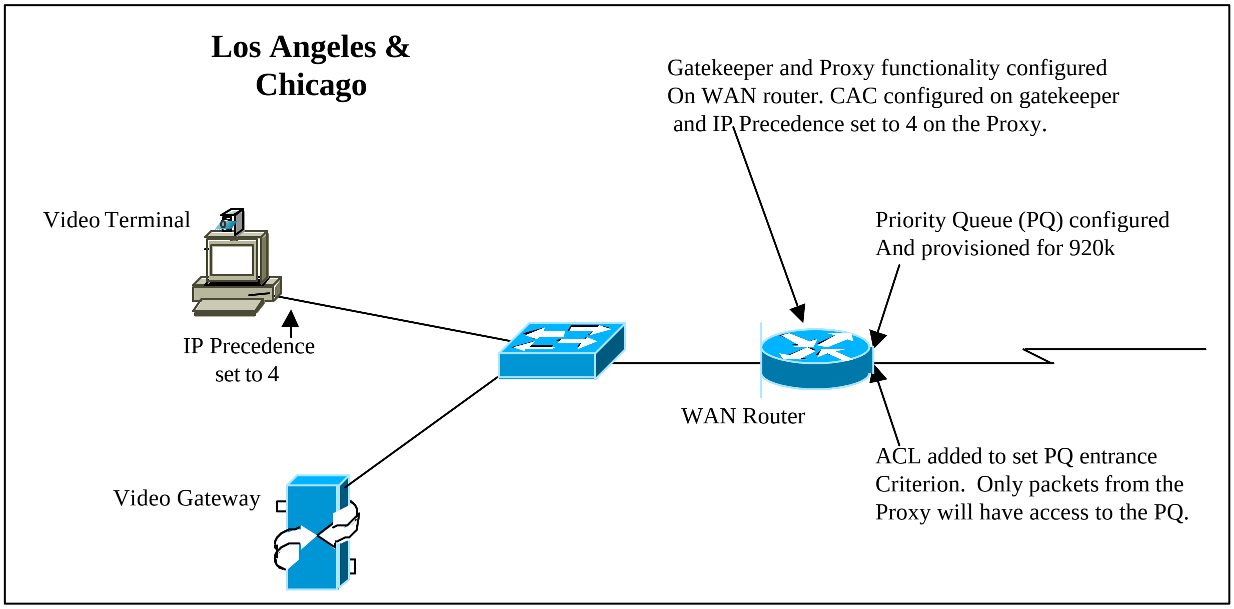

Dallas & Sacramento
Gatekeeper and Proxy functionality configured
On WAN router. CAC configured on gatekeeper
and IP Precedence set to 4 on the Proxy.
Video Terminal
Trust boundaries
configured
Priority Queue (PQ) configured
And provisioned for 920k
IP Precedence
set to 4
WAN Router
MCU or
gateway
IP Precednece
set to 4 and
trust boundary
configured
ACL added to set PQ entrance
Criterion. Only packets from the
Proxy will have access to the PQ.

**Figure 9-5**


Los Angeles &
Chicago
Gatekeeper and Proxy functionality configured
On WAN router. CAC configured on gatekeeper
and IP Precedence set to 4 on the Proxy.
Video Terminal
Priority Queue (PQ) configured
And provisioned for 920k
IP Precedence
set to 4
WAN Router
ACL added to set PQ entrance
Criterion. Only packets from the
Proxy will have access to the PQ.
Video Gateway

# Dial Plan:

When deciding on a dial plan it is always a good idea to start with the incoming PSTN call routing. In our example we have created five zones that all contain video gateways. DID will be used to route incoming calls to video terminals. IVR will be used to route calls from the video gateways in Columbus, Dallas and Sacramento their local MCUs. If for some reason one or more of the zones in our example did not contain a gateway IVR for all-incoming PSTN routing would have been a better choice.

## Zone Prefixes

| Service Prefix | **Zone Prefix** | E.164 Address |
|---|---|---|

The zone prefix for each zone is based on the local area code. Area codes are unique and users are familiar with the number structure. In our configuration there is single zone in each site so the zone prefixes will be based on the area code. If more than one zone were required in a single area code longer zone prefixes could be used (see Zone Prefix Design in Chapeter 6) . The zone prefixes in this network are.

Columbus = 614
Sacramento = 916
Dallas = 972
Chicago = 847
Los Angeles = 213

## Service Prefixes

| **Service Prefix** | Zone Prefix | E.164 Address |
|---|---|---|

Service prefixes must configured for all MCUs and video gateways. As described in Chapter 6 Dial Plans, it is a good idea to reserve a block of numbers for video gateways and a block of numbers for MCUs. In our case the customer has chosen to standardize on 384k calls this makes service prefixes for gateways very simple. The obvious choice would be to use 9 for all PSTN calls, but that would cause routing problems in the Sacramento and Dallas zones. The Sacramento zone prefix is 916, overlapping gateway service prefixes and zone prefixes will cause routing problems. There are two options, reserve another block of numbers other than 9* or use a service prefix such as 9#. In this case we have chosen 9# for PSTN access in all zones. Any time that a user needs to access the WAN the dial string will start with 9#.

For MCU service prefixes 8* will be reserved and the zone prefix will be appended to associate it with the zone the MCU resides in. MCU service prefixes in the Sacramento zone will be 9168*, and in Los Angeles 2128*. Below are the service prefixes chosen for different types of calls on the MCU (these service prefixes will be used in every zone and the zone prefix will be appended).

MCU Service Prefixes:

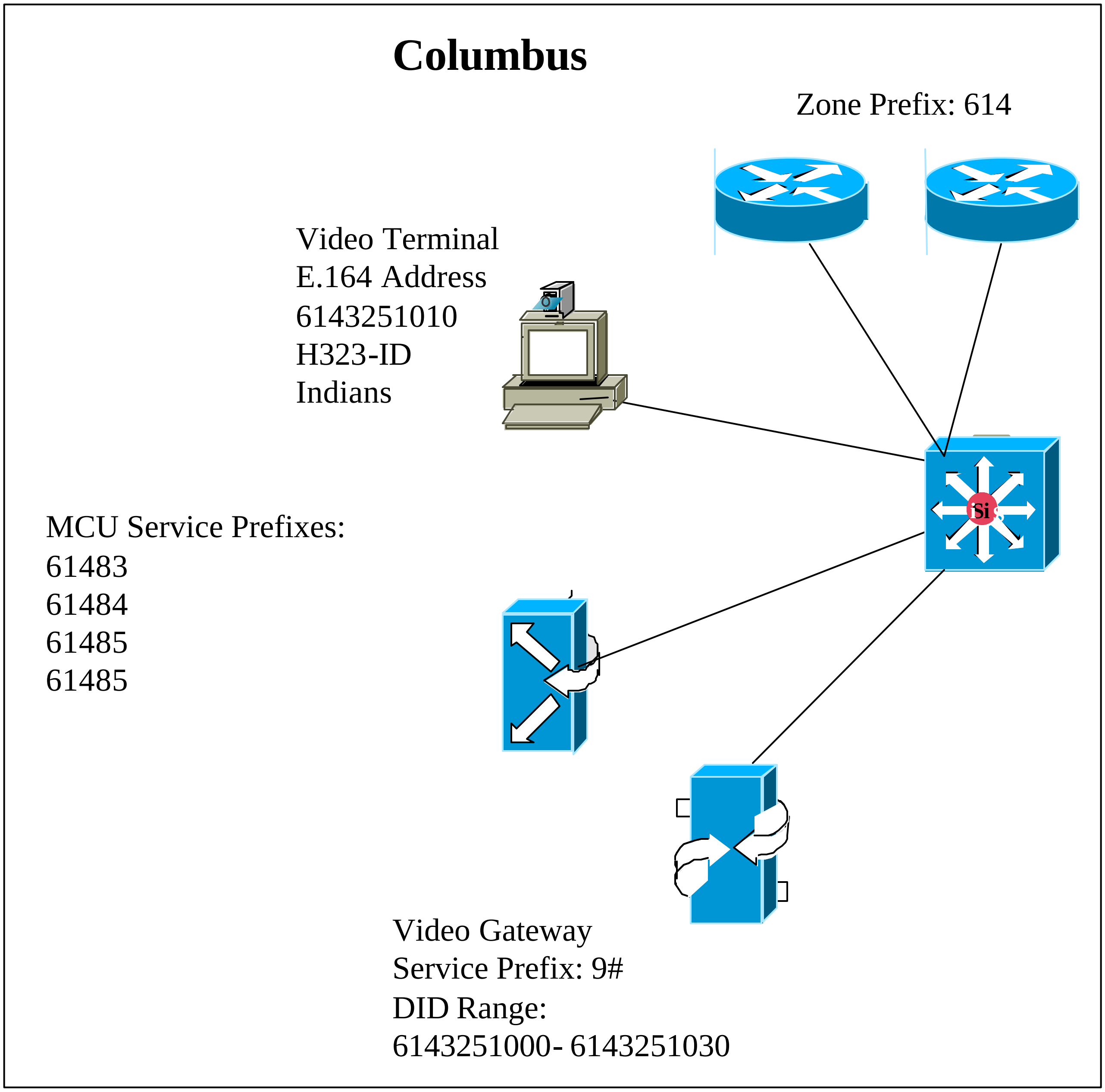
| Service Prefix | Data Rate | Number of Parties | Video Format | Continuous Presence |
|---|---|---|---|---|
| 83 | 384k | 3 | H.261 | No |
| 84 | 384k | 4 | H.261 | Yes |
| 85 | 384k | 5 | H.261 | No |
| 89 | 384k | 9 | H.261 | No |

## E.164 Addresses and H323-ID's

| Service Prefix | Zone Prefix | **E.164 Address** |
|---|---|---|

The carrier will provide E.164 addresses for this customer. Since DID has been chosen for incoming PSTN routing the customer will order blocks of DID numbers with each PRI line. Each video terminal will be assigned a valid DID number for its E.164 address. In Columbus there are 24 video terminals. Thirty DID numbers will be ordered with the PRI line for Columbus (the extra six numbers are for expansion). In Los Angeles and Chicago DID numbers off of the BRI lines will be used as E.164 addresses (see video infrastructure section below for video components at each site). H323-ID's will be based on the conference room name that the system resides in. Since the video terminals may be moved from room to room H323-ID's will not be used for dialing. The customer is using a global address book that will display all of the IP video terminals on the network. Users can choose to dial from the address book, or by manually entering the E.164 address of the unit being called. Figure 9-6 illustrates the Dial plan in Columbus.

**Figure 9-6**


Columbus
Zone Prefix: 614
Video Terminal
E.164 Address
6143251010
H323-ID
Indians
Si
MCU Service Prefixes:
61483
61484
61485
61485
Video Gateway
Service Prefix: 9#
DID Range:
6143251000- 6143251030

## Video Infrastructure:

When deciding on location and number of video components it is important to understand the customer's needs. This customer made it clear that less than ten percent of video calls placed were off net calls. The number of video calls placed daily ranges from 10 to 15 and most calls are multipoint. For this reason the customer decided to go with video gateways at each site, and MCU's in Columbus, Dallas and Sacramento. Below the video components for each site are covered.

### Columbus

- IP Video Terminals 24

  The current 24 H.320 video systems are over three years old and will be replaced with new H.323 group systems that support IP Precedence.

- MCUs 4

  The four MCU's will be configured in a stack allowing one set of service prefixes to be shared by all four MCU's.

- Video Gateway's PRI 1

  A single PRI gateway will be installed with 30 DID numbers that will be assigned to the IP video terminals. All 10 digits will be passed to the gateway by the carrier, allowing each video terminal to register with a 10 digit fully qualified E.164 address. IVR will be enabled and used for PSTN access to MCU conferences. One DID number will need to be reserved for IVR calls.

### Sacramento

- IP Video Terminals 6

  The existing 6 H.320 video systems are over three years old and will be replaced with new H.323 group systems that support IP Precedence.

- MCU 1

  A single MCU will be located on the Sacramento campus for local on site multi point calls. The Sacramento campus is in the process of adding another building and possibly adding two or three additional IP video terminals. The MCU will also allow multiple video terminals to participate in an off campus multipoint call while only consuming the bandwidth of a single call. This will be done by cas cading a Sacramento MCU conference with a Columbus MCU conference.

- Video Gateway 1

  A single PRI gateway will be installed with 10 DID numbers that will be assigned to the IP video terminals. All 10 digits will be passed to the gateway by the carrier, allowing each video terminal to register with a 10 digit fully qualified E.164 address. IVR will also be enabled and used for PSTN access to MCU conferences. One DID number will need to be reserved for IVR calls.

## Dallas

- IP Video Terminals 10

  The existing 10 H.320 video systems are over three years old and will be replaced with new H.323 group systems that support IP Precedence.

- MCU 1

  A single MCU will be located on the Dallas campus for local on site multi point calls. The MCU will also allow multiple video terminals to participate in an off campus multipoint call while only consuming the bandwidth of a single call. This will be done by cascading a Dallas MCU conference with a Columbus MCU conference.

- Video Gateway 1

  A single PRI gateway will be installed with 15 DID numbers that will be assigned to the IP video terminals. All 10 digits will be passed to the gateway by the carrier, allowing each video terminal to register with a 10 digit fully qualified E.164 address. IVR will also be enabled and used for PSTN access to MCU conferences. One DID number will need to be reserved for IVR calls.

## Los Angeles

- IP Video Terminals 4

  The existing 4 H.320 video systems are over three years old and will be replaced with new H.323 group systems that support IP Precedence.

- MCU 0

  Los Angles will not have a local MCU.

- Video Gateway 1

  A single BRI gateway will be installed with four BRI lines. Each video terminal will receive a DID number from one of the BRI lines. IVR will not be enabled on the gateway.

## Chicago

- IP Video Terminals 3

  The existing 3 H.320 video systems are over three years old and will be replaced with new H.323 group systems that support IP Precedence.

- MCU 0

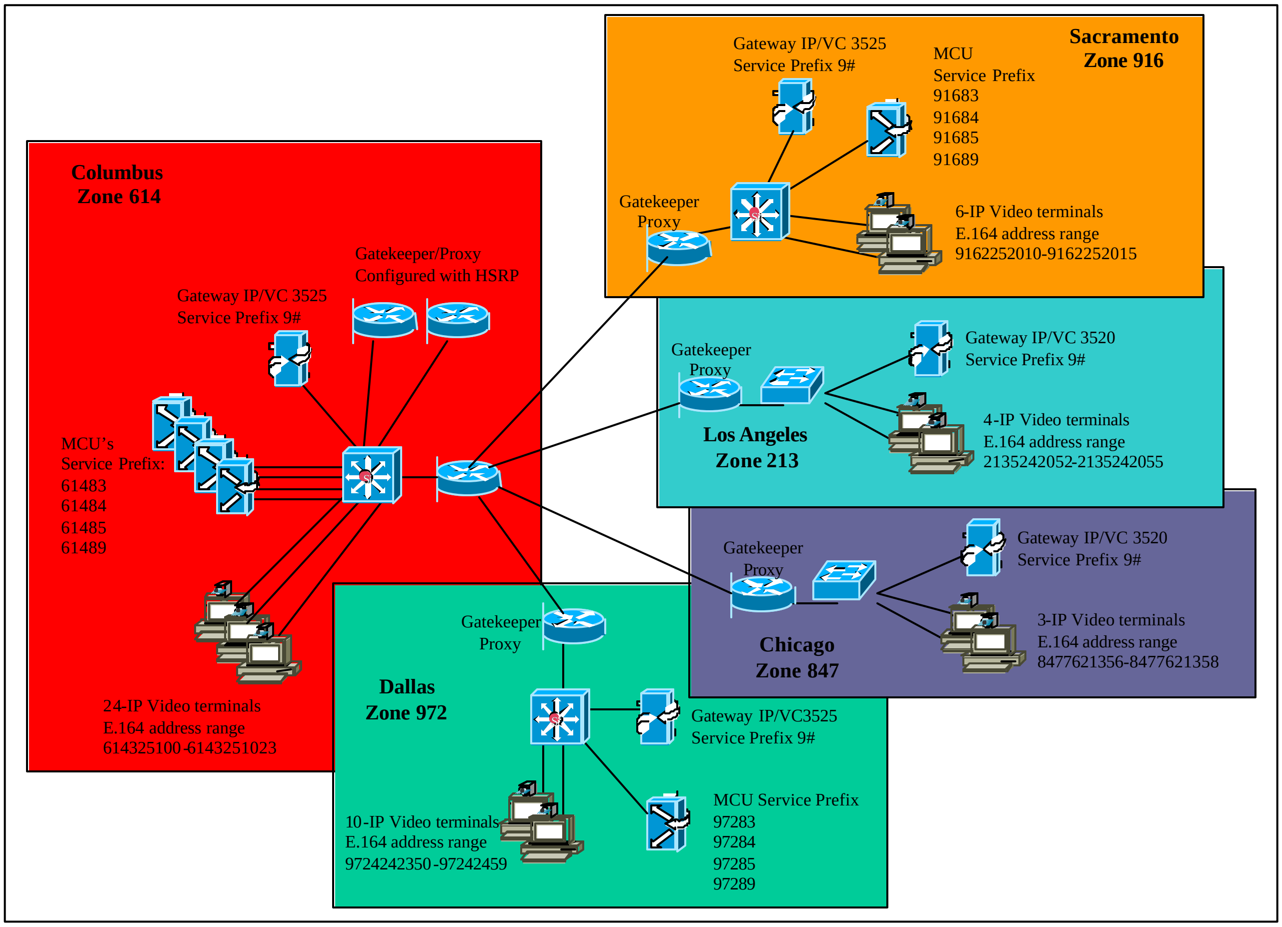
  Chicago will not have a local MCU.

- Video Gateway 1

  A single BRI gateway will be installed with three BRI lines. Each video terminal will receive a DID number from one of the BRI lines. IVR will not be enabled on the gateway.

Figure 9-7 illustrates the video components and dial plan for the new IP video network.

## Figure 9-7



# Glossary:

| | |
|---|---|
| 802.1Q/8021.P | 802.1Q and 802.1P are the standard proposed by the inter-working task groups of the 802 802.1Q is the IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridge Local Area Network (VLAN). 802.1P is the IEEE Standard for Local and Metropolitan Area Networks – Supplement to Media Access Control (MAC) Bridges: Traffic Expending and Dynamic Multicasting Filtering. |
| ARQ | Admission Request |
| AVVID | Architecture for Voice, Video & Integrated Data |
| BRI | Basic Rate Interface |
| CAC | Call Admission Control |
| Cascade | The process of connecting two or more MCUs to create a larger conference |
| CODEC | Code-Decoder for digitizing voice and video. Compression algorithms can also be used during the digitizing process |
| CoS | Class of Service |
| cRTP | Compressed RTP |
| DID | Direct Inward Dial |
| DSCP | Differentiated Services Code Point is an IETF standard that utilizes 6 bits in the Ipv4 header's TOS (Type of Service) field to specify class of service for each packet |
| DTMF | Dual Tone Multifrequency |
| E.164 | Address format used for H.323 devices |
| Gatekeeper | Used for H.323 registration, call routing, and admission control |
| G.711 | G.711 PCM encoding provides 64kbps analog to digital conversion using U-law or A -law |
| H.261 | Video Codec |
| H.263 | Video Codec |
| H.323 | Standard for audio, video, and data communications across IP-based networks |
| H323-ID | Alphanumeric Identifier assigned to an H.323 video terminal |
| Hopoff | Statement added to a Cisco gatekeeper for static Inter zone routing |
| HSRP | Hot Standby Routing Protocol |
| IMUX | Inverse Multiplexer |

| | |
|---|---|
| IP | Internet Protocol |
| IP Precedence | IP Precedence utilizes the three precedence bits in the Ipv4 headers TOS (Type of Service) field to specify class of service for each packet |
| ISDN | Integrated Services Digital Network |
| IVR | Interactive Voice Response |
| LAN | Local Area Network |
| LLQ | Low Latency Queuing; a QoS mechanism that insures the timely queuing of critical, delay sensitive traffic |
| LRQ | Location Request |
| MC | Multipoint controller |
| MCM | Multimedia Conference Manager |
| MCU | Multipoint conference unit used for videoconferences containing more than two endpoints |
| MP | Multipoint processor |
| MSN | Multiple Subscriber Number |
| PRI | Primary Rate Interface |
| Proxy | H.323 to H.323 gateway used for assigning QoS and security access |
| PSTN | Public Switched Telephone Network |
| QoS | Quality of Service |
| RAS | Registration, Admissions and Status |
| RRQ | Registration Request |
| RSVP | Resource Reservation Protocol |
| RTCP | Real-time Control Protocol |
| RTP | Real-time Protocol |
| Service Prefix | A digit string used to identify a service on an MCU or Gateway |
| Stacking | Grouping MCUs to obtain a larger number of multipoint conferences |
| TOS | Type of Service |
| WAN | Wide Area Network |
| WRED | Weighted Random Early Detection |
| WRR | Weighted Round Robin |

Zone A logical group of H.323 Infrastructure components managed by a single gatekeeper.

Zone Prefix A digit string used to identify a group of H.323 devices

## Reference Documents and Links:

T.120 and H.323 Primer:
http://www.databeam.com/standards/index.html

AVVID QoS Guide:

http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/avvidqos/index.htm